

- [243] D. KOZEN. Results on the propositional  $\mu$ -calculus. *Theoretical Computer Science*, **27**:333–354, 1983.
- [244] S. A. KRIPKE. Semantical considerations on modal logic. *Acta Philosophica Fennica*, **16**:83–94, 1963.
- [245] F. KRÖGER. *Temporal Logic of Programs*, volume 8 of *Springer Monographs on Theoretical Computer Science*. Springer-Verlag, 1987.
- [246] T. KROPF. *Introduction to Formal Hardware Verification*. Springer-Verlag, 1999.
- [247] A. KUCERA AND P. SCHNOEBELEN. A general approach to comparing infinite-state systems with their finite-state specifications. *Theoretical Computer Science*, **358**(2-3):315–333, 2006.
- [248] V. KULKARNI. *Modeling and Analysis of Stochastic Systems*. Chapman & Hall, 1995.
- [249] O. KUPFERMAN AND M.Y. VARDI. Model checking of safety properties. *Formal Methods in System Design*, **19**(3):291–314, 2001.
- [250] R. KURSHAN. *Computer-aided Verification of Coordinating Processes: The Automata-Theoretic Approach*. Princeton University Press, 1994.
- [251] R. KURSHAN AND V. LEVIN AND M. MINEA AND D. PELED AND H. YENIGÜN. Combining software and hardware verification techniques. *Formal Methods in System Design*, **21**(3):251–280, 2002.
- [252] M. KWIATKOWSKA. Survey of fairness notions. *Information and Software Technology*, **31**(7):371–386, 1989.
- [253] M. KWIATKOWSKA. A metric for traces. *Information Processing Letters*, **35**(3):129–135, 1990.
- [254] M. KWIATKOWSKA AND G. NORMAN AND D. PARKER. Modelling and verification of probabilistic systems. In P. Panangaden and F. van Breugel, editors, *Part 2 of Mathematical Techniques for Analyzing Concurrent and Probabilistic Systems*, volume 23 of *CRM Monograph Series*. AMS Press, 2004.
- [255] M. KWIATKOWSKA AND G. NORMAN AND D. PARKER. Probabilistic symbolic model checking with PRISM: A hybrid approach. *International Journal on Software Tools for Technology Transfer*, **6**(2):128–142, 2004.
- [256] L. LAMPORT. A new solution of Dijkstra’s concurrent programming problem. *Communications of the ACM*, **17**(8):453–455, 1974.

- [257] L. LAMPORT. Proving the correctness of multiprocess programs. *IEEE Transactions on Software Engineering*, **3**(2):125–143, 1977.
- [258] L. LAMPORT. Time, clocks and the ordering of events in distributed systems. *Communication of the ACM*, **21**(7):558–565, 1978.
- [259] L. LAMPORT. “Sometime” is sometimes “not never” – on the temporal logic of programs. In *7th Annual Symposium on Principles of Programming Languages (POPL)*, pages 174–185. ACM Press, 1980.
- [260] L. LAMPORT. The temporal logic of actions. *ACM Transactions on Programming Languages and Systems*, **16**(3):872–923, 1994.
- [261] L. H. LANDWEBER. Decision problems for omega-automata. *Mathematical Systems Theory*, **3**(4):376–384, 1969.
- [262] F. LAROUSSINIE AND N. MARKAY AND PH. SCHNOEBELEN. Temporal logic with forgettable past. In *17th IEEE Symposium on Logic in Computer Science (LICS)*, pages 383–392. IEEE Computer Society Press, 2002.
- [263] K. G. LARSEN AND J. PEARSON AND C. WEISE AND W. YI. Clock difference diagrams. *Nordic Journal of Computing*, **6**(3):271–298, 1999.
- [264] K. G. LARSEN AND A. SKOU. Bisimulation through probabilistic testing. *Information and Computation*, **94**(1):1–28, 1991.
- [265] K. G. LARSEN AND W. YI. Time-abstracted bisimulation: implicit specification and decidability. In *9th International Conference on the Mathematical Foundations of Programming Semantics (MFPS)*, volume 802 of *Lecture Notes in Computer Science*, pages 160–176. Springer-Verlag, 1993.
- [266] D. LEE AND M. YANNAKAKIS. Online minimization of transition systems. In *24th Annual ACM Symposium on Theory of Computing (STOC)*, pages 264–274. ACM Press, 1992.
- [267] D. LEHMANN AND A. PNUELI AND J. STAVI. Impartiality, justice and fairness: the ethics of concurrent termination. In *8th Colloquium on Automata, Languages and Programming (ICALP)*, volume 115 of *Lecture Notes in Computer Science*, pages 264–277. Springer-Verlag, 1981.
- [268] D. LEHMANN AND M. RABIN. On the advantages of free choice: a symmetric and fully distributed solution to the dining philosophers problem. In *8th ACM Symposium on Principles of Programming Languages (POPL)*, pages 133–138. ACM Press, 1981.
- [269] N. LEVESON. *Safeware: System Safety and Computers*. ACM Press, 1995.

- [270] C. LEWIS. Implication and the algebra of logic. *Mind*, **N. S.**, **12**(84):522–531, 1912.
- [271] H. R. LEWIS. A logic of concrete time intervals (extended abstract). In *5th Annual IEEE Symposium on Logic in Computer Science (LICS)*, pages 380–389. IEEE Computer Society Press, 1990.
- [272] H. R. LEWIS AND C. H. PAPADIMITRIOU. *Elements of the Theory of Computation*. Prentice-Hall, 1997.
- [273] O. LICHTENSTEIN AND A. PNUELI. Checking that finite-state concurrent programs satisfy their linear specification. In *12th Annual ACM Symposium on Principles of Programming Languages (POPL)*, pages 97–107. ACM Press, 1985.
- [274] O. LICHTENSTEIN AND A. PNUELI AND L. ZUCK. The glory of the past. In *Conference on Logic of Programs*, volume 193 of *Lecture Notes in Computer Science*, pages 196–218. Springer-Verlag, 1985.
- [275] P. LIGGESMEYER AND M. ROTHFELDER AND M. RETTELBACH AND T. ACKERMANN. Qualitätssicherung Software-basierter technischer Systeme. *Informatik Spektrum*, **21**(5):249–258, 1998.
- [276] R. LIPTON. Reduction: a method of proving properties of parallel programs. *Communications of the ACM*, **18**(12):717–721, 1975.
- [277] C. LOISEAUX AND S. GRAF AND J. SIFAKIS AND A. BOUAJJANI AND S. BENSELEM. Property preserving abstractions for the verification of concurrent systems. *Formal Methods in System Design*, **6**(1):11–44, 1995.
- [278] G. LOWE. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. *Software Concepts and Tools*, **17**(3):93–102, 1996.
- [279] N. LYNCH AND F. VAANDRAGER. Forward and backward simulations – part I: untimed systems. *Information and Computation*, **121**(2):214–233, 1993.
- [280] N. A. LYNCH. *Distributed Algorithms*. Morgan Kaufmann Publishers, 1996.
- [281] O. MALER AND Z. MANNA AND A. PNUELI. From timed to hybrid systems. In *Real-Time: Theory in Practice, REX Workshop*, volume 600 of *Lecture Notes in Computer Science*, pages 447–484. Springer-Verlag, 1992.
- [282] Z. MANNA AND A. PNUELI. Completing the temporal picture. *Theoretical Computer Science*, **83**(1):97–130, 1991.
- [283] Z. MANNA AND A. PNUELI. *The Temporal Logic of Reactive and Concurrent Systems: Specification*. Springer-Verlag, 1992.

- [284] Z. MANNA AND A. PNUELI. *The Temporal Logic of Reactive and Concurrent Systems: Safety*. Springer-Verlag, 1995.
- [285] P. MANOLIOS AND R. TREFLER. Safety and liveness in branching time. In *16th Annual IEEE Symposium on Logic in Computer Science (LICS)*, pages 366–372. IEEE Computer Society Press, 2001.
- [286] P. MANOLIOS AND R. J. TREFLER. A lattice-theoretic characterization of safety and liveness. In *22nd Annual Symposium on Principles of Distributed Computing (PODC)*, pages 325–333. IEEE Computer Society Press, 2003.
- [287] A. MAZURKIEWICZ. Trace theory. In *Advances in Petri Nets*, volume 255 of *Lecture Notes in Computer Science*, pages 279–324. Springer-Verlag, 1987.
- [288] K. L. McMILLAN. *Symbolic Model Checking*. Kluwer Academic Publishers, 1993.
- [289] K. L. McMILLAN. A technique of state space search based on unfoldings. *Formal Methods in System Design*, **6**(1):45–65, 1995.
- [290] R. McNAUGHTON. Testing and generating infinite sequences by a finite automaton. *Information and Control*, **9**(5):521–530, 1966.
- [291] G. H. MEALY. A method for synthesizing sequential circuits. *Bell System Technical Journal*, **34**:1045–1079, 1955.
- [292] C. MEINEL AND T. THEOBALD. *Algorithms and Data Structures in VLSI Design*. Springer-Verlag, 1998.
- [293] S. MERZ. Model checking: a tutorial. In F. Cassez, C. Jard, B. Rozoy, and M.D. Ryan, editors, *Modelling and Verification of Parallel Processes*, volume 2067 of *Lecture Notes in Computer Science*, pages 3–38. Springer-Verlag, 2001.
- [294] S. MERZ AND N. NAVET (EDITORS). *Modeling and Verification of Real-Time Systems: Formalisms and Software Tools*. ISTE Ltd, 2008.
- [295] R. MILNER. An algebraic definition of simulation between programs. In *2nd International Joint Conference on Artificial Intelligence*, pages 481–489. William Kaufmann, 1971.
- [296] R. MILNER. *A Calculus of Communicating Systems*, volume 92 of *Lecture Notes in Computer Science*. Springer-Verlag, 1980.
- [297] R. MILNER. Calculi for synchrony and asynchrony. *Theoretical Computer Science*, **25**(3):267–310, 1983.
- [298] R. MILNER. *Communication and Concurrency*. Prentice-Hall, 1989.

- [299] R. MILNER. *Communicating and Mobile Systems: The Pi-Calculus*. Cambridge University Press, 1999.
- [300] S. MINATO. *Binary Decision Diagrams and Applications for VLSI CAD*. Kluwer Academic Publishers, 1996.
- [301] S. MINATO AND N. ISHIURA AND S. YAJIMA. Shared binary decision diagram with attributed edges for efficient boolean function manipulation. In *27th ACM/IEEE Conference on Design Automation (DAC)*, pages 52–57. ACM Press, 1991.
- [302] F. MOLLER AND S. A. SMOLKA. On the computational complexity of bisimulation. *ACM Computing Surveys*, **27**(2):287–289, 1995.
- [303] E. F. MOORE. Gedanken-experiments on sequential machines. *Automata Studies*, **34**:129–153, 1956.
- [304] C. MORGAN AND A. MCIVER. pGCL: Formal reasoning for random algorithms. *South African Computer Journal*, **22**:14–27, 1999.
- [305] A. W. MOSTOWSKI. Regular expressions for infinite trees and a standard form of automata. In *5th Symposium on Computational Theory*, volume 208 of *Lecture Notes in Computer Science*, pages 157–168. Springer-Verlag, 1984.
- [306] R. MOTWANI AND P. RAGHAVAN. *Randomized Algorithms*. Cambridge University Press, 1995.
- [307] D. E. MULLER. Infinite sequences and finite machines. In *4th IEEE Symposium on Switching Circuit Theory and Logical Design*, pages 3–16. IEEE, 1963.
- [308] G. J. MYERS. *The Art of Software Testing*. John Wiley & Sons, 1979.
- [309] J. MYHILL. Finite automata and the representation of events. Technical Report WADD TR-57-624, Wright Patterson Air Force Base, OH, 1957.
- [310] R. NALUMASU AND G. GOPALAKRISHNAN. A new partial order reduction algorithm for concurrent systems. In *Thirteenth IFIP International Conference on Hardware Description Languages and their Applications (CHDL)*, pages 305–314. Chapman & Hall, 1997.
- [311] K. S. NAMJOSHI. A simple characterization of stuttering bisimulation. In *17th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS)*, volume 1346 of *Lecture Notes in Computer Science*, pages 284–296. Springer-Verlag, 1997.
- [312] G. NAUMOVICH AND L. A. CLARKE. Classifying properties: an alternative to the safety-liveness classification. *ACM SIGSOFT Software Engineering Notes*, **25**(6):159–168, 2000.

- [313] A. NERODE. Linear automaton transformations. In *Proceedings of the American Mathematical Society*, volume 9, pages 541–544, 1958.
- [314] R. DE NICOLA AND F. VAANDRAGER. Three logics for branching bisimulation (extended abstract). In *5th Annual IEEE Symposium on Logic in Computer Science (LICS)*, pages 118–129. IEEE Computer Society Press, Springer-Verlag, 1990.
- [315] X. NICOLLIN AND J.-L. RICHIER AND J. SIFAKIS AND J. VOIRON. ATP: an algebra for timed processes. In *IFIP TC2 Working Conference on Programming Concepts and Methods*, pages 402–427. North Holland, 1990.
- [316] A. OLIVERO AND J. SIFAKIS AND S. YOVINE. Using abstractions for the verification of linear hybrid systems. In *6th International Conference on Computer Aided Verification (CAV)*, volume 818 of *Lecture Notes in Computer Science*, pages 81–94. Springer-Verlag, 1994.
- [317] S. OWICKI. Verifying concurrent programs with shared data classes. In *IFIP Working Conference on Formal Description of Programming Concepts*, pages 279–298. North Holland, 1978.
- [318] R. PAIGE AND R. E. TARJAN. Three partition refinement algorithms. *SIAM Journal on Computing*, **16**(6):973–989, 1987.
- [319] P. PANANGADEN. Measure and probability for concurrency theorists. *Theoretical Computer Science*, **253**(2):287–309, 2001.
- [320] C. PAPADIMITRIOU. *Computational Complexity*. Addison-Wesley, 1994.
- [321] D. PARK. On the semantics of fair parallelism. In *Abstract Software Specification*, volume 86 of *Lecture Notes in Computer Science*, pages 504–526. Springer-Verlag, 1979.
- [322] D. PARK. Concurrency and automata on infinite sequences. In *5th GI-Conference on Theoretical Computer Science*, volume 104 of *Lecture Notes in Computer Science*, pages 167–183. Springer-Verlag, 1981.
- [323] D. PARKER. *Implementation of Symbolic Model Checking for Probabilistic Systems*. PhD thesis, University of Birmingham, UK, 2002.
- [324] D. PELED. All from one, one for all: On model checking using representatives. In *5th International Conference on Computer Aided Verification (CAV)*, volume 697 of *Lecture Notes in Computer Science*, pages 409–423. Springer-Verlag, 1993.
- [325] D. PELED. Combining partial order reductions with on-the-fly model checking. *Formal Methods in System Design*, **8**(1):39–64, 1996.

- [326] D. PELED. Partial order reduction: Linear and branching temporal logics and process algebras. In *Partial Order Methods in Verification* [328], pages 79–88.
- [327] D. PELED. *Software Reliability Methods*. Springer-Verlag, 2001.
- [328] D. PELED AND V. PRATT AND G. J. HOLZMANN (EDITORS). *Partial Order Methods in Verification*, volume 29 (10) of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*. AMS Press, 1997.
- [329] D. PELED AND T. WILKE. Stutter-invariant temporal properties are expressible without the next-time operator. *Information Processing Letters*, **63**(5):243–246, 1997.
- [330] W. PENCZEK AND R. GERTH AND R. KUIPER AND M. SZRETER. Partial order reductions preserving simulations. In *8th Workshop on Concurrency, Specification and Programming (CS&P)*, pages 153–172. Warsaw University Press, 1999.
- [331] G. DELLA PENNA AND B. INTRIGILA AND I. MELATTI AND E. TRONCI AND M. VENTURINI ZILLI. Finite horizon analysis of Markov chains with the Murphi verifier. *Journal on Software Tools and Technology Transfer*, **8**(4-5):397–409, 2006.
- [332] G. L. PETERSON. Myths about the mutual exclusion problem. *Information Processing Letters*, **12**(3):15–116, 1981.
- [333] J. L. PETERSON. *Petri Net Theory and the Modeling of Systems*. Prentice-Hall, 1981.
- [334] G. D. PLOTKIN. A structural approach to operational semantics. Technical Report DAIMI FN-19, Aarhus University, 1981.
- [335] G. D. PLOTKIN. The origins of structural operational semantics. *Journal of Logic and Algebraic Programming*, **60–61**:3–15, 2005.
- [336] G. D. PLOTKIN. A structural approach to operational semantics. *Journal of Logic and Algebraic Programming*, **60–61**:17–139, 2005.
- [337] A. PNUELI. The temporal logic of programs. In *18th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 46–67. IEEE Computer Society Press, 1977.
- [338] A. PNUELI. Linear and branching structures in the semantics and logics of reactive systems. In *12th International Colloquium on Automata, Languages and Programming (ICALP)*, volume 194 of *Lecture Notes in Computer Science*, pages 15–32. Springer-Verlag, 1985.

- [339] A. PNUELI. Applications of temporal logic to the specification and verification of reactive systems: a survey of current trends. In *Advanced School on Current Trends in Concurrency Theory*, volume 244 of *Lecture Notes in Computer Science*, pages 510–584. Springer-Verlag, 1986.
- [340] A. PNUELI AND L. ZUCK. Probabilistic verification by tableaux. In *1st Annual Symposium on Logic in Computer Science (LICS)*, pages 322–331. IEEE Computer Society Press, 1986.
- [341] A. PNUELI AND L. ZUCK. Probabilistic verification. *Information and Computation*, **103**(1):1–29, 1993.
- [342] H. POSPESEL. *Introduction to Logic: Propositional Logic*. Prentice-Hall, 1979.
- [343] V. PRATT. Modelling concurrency with partial orders. *International Journal of Parallel Programming*, **15**(1):33–71, 1986.
- [344] W. PRESS AND S. A. TEUKOLSKY AND W. T. VETTERLING AND B. P. FLANNERY. *Numerical Recipes in C++. The Art of Scientific Computing*. Cambridge University Press, 2002.
- [345] A. PRIOR. *Time and Modality*. Oxford University Press, 1957.
- [346] M. PUTERMAN. *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. John Wiley & Sons, 1994.
- [347] J.-P. QUEILLE AND J. SIFAKIS. Specification and verification of concurrent systems in CESAR. In *5th International Symposium on Programming*, volume 137 of *Lecture Notes in Computer Science*, pages 337–351. Springer-Verlag, 1982.
- [348] J.-P. QUEILLE AND J. SIFAKIS. Fairness and related properties in transition systems. a temporal logic to deal with fairness. *Acta Informatica*, **19**(3):195–220, 1983.
- [349] M. O. RABIN. Probabilistic algorithms. In J. F. Traub, editor, *Algorithms and Complexity: New Directions and Recent Results*, pages 21–39. Academic Press, 1976.
- [350] M. O. RABIN AND D. SCOTT. Finite automata and their decision problems. *IBM Journal of Research and Development*, **3**(2):114–125, 1959.
- [351] M.O. RABIN. Decidability of second order theories and automata on infinite trees. *Transactions of the AMS*, **141**:1–35, 1969.
- [352] Y. RAMAKRISHNA AND S. SMOLKA. Partial-order reduction in the weak modal mu-calculus. In *8th International Conference on Concurrency Theory (CONCUR)*, volume 1243 of *Lecture Notes in Computer Science*, pages 5–24. Springer-Verlag, 1997.



- [353] J. I. RASMUSSEN AND K. G. LARSEN AND K. SUBRAMANI. On using priced timed automata to achieve optimal scheduling. *Formal Methods in System Design*, **29**(1):97–114, 2006.
- [354] M. REM. Trace theory and systolic computations. In *Parallel Architectures and Languages Europe (PARLE)*, volume 1, volume 258 of *Lecture Notes in Computer Science*, pages 14–33. Springer-Verlag, 1987.
- [355] M. REM. A personal perspective of the Alpern-Schneider characterization of safety and liveness. In W. H. J. Feijen, A. J. M. van Gasteren, D. Gries, and J. Misra, editors, *Beauty is Our Business: A Birthday Salute to Edsger W. Dijkstra*, chapter 43, pages 365–372. Springer-Verlag, 1990.
- [356] A. W. ROSCOE. Model-checking CSP. In A. W. Roscoe, editor, *A Classical Mind: Essays in Honour of C. A. R. Hoare*, pages 353–378. Prentice-Hall, 1994.
- [357] G. ROZENBERG AND V. DIEKERT. *The Book of Traces*. World Scientific Publishing Co., Inc., 1995.
- [358] R. RUDELL. Dynamic variable ordering for ordered binary decision diagrams. In *International Conference on Computer-Aided Design (ICCAD)*, pages 42–47. IEEE Computer Society Press, 1993.
- [359] J. RUSHBY. Formal methods and the certification of critical systems. Technical Report SRI-CSL-93-7, SRI International, 1993. (also issued as *Formal Methods and Digital System Validation*, NASA CR 4551).
- [360] T. C. RUYS AND E. BRINKSMA. Managing the verification trajectory. *International Journal on Software Tools for Technology Transfer*, **4**(2):246–259, 2003.
- [361] S. SAFRA. On the complexity of  $\omega$ -automata. In *29th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 319–327. IEEE Computer Society Press, 1988.
- [362] A. L. SANGIOVANNI-VINCENTELLI AND P. C. MCGEER AND A. SALDANHA. Verification of electronic systems. In *33rd Annual Conference on Design Automation (DAC)*, pages 106–111. ACM Press, 1996.
- [363] J. E. SAVAGE. *Models of Computation: Exploring the Power of Computing*. Addison-Wesley, 1998.
- [364] T. SCHLIPF AND T. BUECHNER AND R. FRITZ AND M. HELMS AND J. KOEHL. Formal verification made easy. *IBM Journal of Research and Development*, **41**(4–5):567–576, 1997.
- [365] K. SCHNEIDER. *Verification of Reactive Systems: Formal Methods and Algorithms*. Springer-Verlag, 2004.

- [366] S. SCHNEIDER. *Specifying Real-Time Systems in Timed CSP*. Prentice-Hall, 2000.
- [367] A. SCHRIJVER. *Combinatorial Optimization: Polyhedra and Efficiency*. Springer, 2003.
- [368] S. SCHWOON AND J. ESPARZA. A note on on-the-fly verification algorithms. In *11th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, volume 3440 of *Lecture Notes in Computer Science*, pages 174–190. Springer-Verlag, 2005.
- [369] R. SEBASTIANI AND S. TONETTA. “More deterministic” vs. “smaller” Büchi automata for efficient LTL model checking. In *12th Advanced Research Working Conference on Correct Hardware Design and Verification Methods (CHARME)*, volume 2860 of *Lecture Notes in Computer Science*, pages 126–140. Springer-Verlag, 2003.
- [370] R. SEGALA AND N. LYNCH. Probabilistic simulations for probabilistic processes. *Nordic Journal of Computing*, **2**(2):250–273, 1995.
- [371] A. P. SISTLA. Safety, liveness and fairness in temporal logic. *Formal Aspects of Computing*, **6**(5):495–512, 1994.
- [372] A. P. SISTLA AND E. M. CLARKE. The complexity of propositional linear temporal logic. *Journal of the ACM*, **32**(3):733–749, 1985.
- [373] A. P. SISTLA AND M. Y. VARDI AND P. WOLPER. The complementation problem for Büchi automata with applications to temporal logic. *Theoretical Computer Science*, **49**:217–237, 1987.
- [374] F. SOMENZI. Binary decision diagrams. In M. Broy and R. Steinbruggen, editors, *Calculational System Design*, volume 173 of *NATO Science Series F: Computer and Systems Sciences*, pages 303–366. IOS Press, 1999.
- [375] F. SOMENZI AND R. BLOEM. Efficient Büchi automata from LTL formulae. In *12th International Conference on Computer Aided Verification (CAV)*, volume 1855 of *Lecture Notes in Computer Science*, pages 248–263. Springer-Verlag, 2000.
- [376] L. STAIGER. Research in the theory of omega-languages. *Elektronische Informationsverarbeitung und Kybernetik*, **23**(8–9):415–439, 1987.
- [377] J. STAUNSTRUP AND H. R. ANDERSEN AND H. HULGAARD AND J. LIND-NIELSEN AND K. G. LARSEN AND G. BEHRMANN AND K. KRISTOFFERSEN AND A. SKOU AND H. LEERBERG AND N. B. THEILGAARD. Practical verification of embedded software. *IEEE Computer*, **33**(5):68–75, 2000.
- [378] W. J. STEWART. *Introduction to the Numerical Solution of Markov Chains*. Princeton University Press, 1994.

- [379] C. STIRLING. *Modal and Temporal Properties of Processes*. Texts in Computer Science. Springer-Verlag, New York, 2001.
- [380] F. A. STOMP AND W.-P. DE ROEVER. A principle for sequential reasoning about distributed algorithms. *Formal Aspects of Computing*, **6**(6):716–737, 1994.
- [381] N. STOREY. *Safety-Critical Computer Systems*. Addison-Wesley, 1996.
- [382] R. S. STREETT. Propositional dynamic logic of looping and converse is elementarily decidable. *Information and Control*, **54**(1–2):121–141, 1982.
- [383] T. A. SUDKAMP. *Languages and Machines, 3rd edition*. Addison-Wesley, 2005.
- [384] B.K. SZYMANSKI. A simple solution to Lamport’s concurrent programming problem with linear wait. In *International Conference on Supercomputing Systems*, pages 621–626, 1988.
- [385] L. TAN AND R. CLEAVELAND. Simulation revisited. In *7th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, volume 2031 of *Lecture Notes in Computer Science*, pages 480–495. Springer-Verlag, 2001.
- [386] S. TANI AND K. HAMAGUCHI AND S. YAJIMA. The complexity of the optimal variable ordering problems of shared binary decision diagrams. In *4th International Symposium on Algorithms and Computation*, volume 762 of *Lecture Notes in Computer Science*, pages 389–398. Springer-Verlag, 1993.
- [387] R. TARJAN. Depth-first search and linear graph algorithms. *SIAM Journal on Computing*, **1**(2):146–160, 1972.
- [388] H. TAURIAINEN. Nested emptiness search for generalized Büchi automata. Research Report A79, Helsinki University of Technology, Laboratory for Theoretical Computer Science, 2003.
- [389] X. THIRIOUX. Simple and efficient translation from LTL formulas to Büchi automata. *Electronic Notes in Theoretical Computer Science*, **66**(2), 2002.
- [390] W. THOMAS. Automata on infinite objects. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B: Formal Models and Semantics, chapter 4, pages 133–191. Elsevier Publishers B.V., 1990.
- [391] W. THOMAS. Languages, automata, and logic. In G. Rozenberg and A. Salomaa, editors, *Handbook of Formal Languages*, volume 3, pages 389–455. Springer-Verlag, 1997.
- [392] B. A. TRAKHTENBROT. Finite automata and the logic of one-place predicates. *Siberian Mathematical Journal*, **3**:103–131, 1962.

- [393] G. J. TRETMAANS AND K. WIJBRANS AND M. CHAUDRON. Software engineering with formal methods: the development of a storm surge barrier control system. *Formal Methods in System Design*, **19**(2):195–215, 2001.
- [394] S. TRIPAKIS AND S. YOVINE. Analysis of timed systems based on time-abstracting bisimulations. In *8th International Conference on Computer Aided Verification (CAV)*, volume 1102 of *Lecture Notes in Computer Science*, pages 232–243. Springer-Verlag, 1996.
- [395] S. TRIPAKIS AND S. YOVINE. Analysis of timed systems using time-abstracting bisimulations. *Formal Methods in System Design*, **18**(1):25–68, 2001.
- [396] R. TRUDEAU. *Introduction to Graph Theory*. Dover Publications Inc., 1994.
- [397] D. TURI AND J. J. M. M. RUTTEN. On the foundations of final coalgebra semantics. *Mathematical Structures in Computer Science*, **8**(5):481–540, 1998.
- [398] A. VALMARI. Stubborn sets for reduced state space generation. In *10th International Conference on Applications and Theory of Petri Nets (ICATPN)*, volume 483 of *Lecture Notes in Computer Science*, pages 491–515. Springer-Verlag, 1989.
- [399] A. VALMARI. A stubborn attack on state explosion. *Formal Methods in System Design*, **1**(4):297–322, 1992.
- [400] A. VALMARI. On-the-fly verification with stubborn sets. In *5th International Conference on Computer Aided Verification (CAV)*, volume 697 of *Lecture Notes in Computer Science*, pages 397–408. Springer-Verlag, 1993.
- [401] A. VALMARI. Stubborn set methods for process algebras. In *Partial Order Methods in Verification* [328], pages 213–231.
- [402] H. VAN DER SCHOOT AND H. URAL. An improvement of partial order verification. *Software Testing, Verification and Reliability*, **8**(2):83–102, 1998.
- [403] J.L.A. VAN DER SNEPSCHEUT. *Trace Theory and VLSI Design*, volume 200 of *Lecture Notes in Computer Science*. Springer-Verlag, 1985.
- [404] R. J. VAN GLABBEEK. The linear time – branching time spectrum (extended abstract). In *1st International Conference on Concurrency Theory (CONCUR)*, volume 458 of *Lecture Notes in Computer Science*, pages 278–297. Springer-Verlag, 1990.
- [405] R. J. VAN GLABBEEK. The linear time – branching time spectrum II. In *4th International Conference on Concurrency Theory (CONCUR)*, volume 715 of *Lecture Notes in Computer Science*, pages 66–81. Springer-Verlag, 1993.
- [406] R. J. VAN GLABBEEK AND W. P. WEIJLAND. Branching time and abstraction in bisimulation semantics. *Journal of the ACM*, **43**(3):555–600, 1996.

- [407] M. Y. VARDI. Automatic verification of probabilistic concurrent finite-state programs. In *26th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 327–338. IEEE Computer Society Press, 1985.
- [408] M. Y. VARDI. An automata-theoretic approach to linear temporal logic. In *8th Banff Higher Order Workshop Conference on Logics for Concurrency: Structure versus Automata*, volume 1043 of *Lecture Notes in Computer Science*, pages 238–266. Springer-Verlag, 1996.
- [409] M. Y. VARDI. Probabilistic linear-time model checking: An overview of the automata-theoretic approach. In *5th International AMAST Workshop on Formal Methods for Real-Time and Probabilistic Systems (ARTS)*, volume 1601, pages 265–276. Springer-Verlag, 1999.
- [410] M. Y. VARDI. Branching versus linear time: Final showdown. In *7th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, volume 2031 of *Lecture Notes in Computer Science*, pages 1–22. Springer-Verlag, 2001.
- [411] M. Y. VARDI AND P. WOLPER. An automata-theoretic approach to automatic program verification (preliminary report). In *1st Annual Symposium on Logic in Computer Science (LICS)*, pages 332–344. IEEE Computer Society Press, 1986.
- [412] M. Y. VARDI AND P. WOLPER. Reasoning about infinite computations. *Information and Computation*, **115**(1):1–37, 1994.
- [413] K. VARPAANIEMI. On stubborn sets in the verification of linear time temporal properties. In *19th International Conference on Application and Theory of Petri Nets (ICATPN)*, volume 1420 of *Lecture Notes in Computer Science*, pages 124–143. Springer-Verlag, 1998.
- [414] W. VISSER AND H. BARRINGER. Practical CTL\* model checking: should SPIN be extended? *International Journal on Software Tools for Technology Transfer*, **2**(4):350–365, 2000.
- [415] H. VÖLZER AND D. VARACCA AND E. KINDLER. Defining fairness. In *16th International Conference on Concurrency Theory (CONCUR)*, volume 3653 of *Lecture Notes in Computer Science*, pages 458–472. Springer-Verlag, 2005.
- [416] F. WALLNER. Model checking LTL using net unfoldings. In *10th International Conference on Computer Aided Verification (CAV)*, volume 1427 of *Lecture Notes in Computer Science*, pages 207–218. Springer-Verlag, 1998.
- [417] F. WANG. Efficient verification of timed automata with BDD-like data structures. *Journal on Software Tools and Technology Transfer*, **6**(1):77–97, 2004.

- [418] I. WEGENER. *Branching Programs and Binary Decision Diagrams: Theory and Applications*. SIAM Monographs on Discrete Mathematics and Applications. Society for Industrial and Applied Mathematics, 2000.
- [419] C. H. WEST. An automated technique for communications protocol validation. *IEEE Transactions on Communications*, **26**(8):1271–1275, 1978.
- [420] C. H. WEST. Protocol validation in complex systems. In *Symposium on Communications Architectures and Protocols*, pages 303–312. ACM Press, 1989.
- [421] J. A. WHITTAKER. What is software testing? Why is it so hard? *IEEE Software*, **17**(1):70–79, 2000.
- [422] B. WILLEMS AND P. WOLPER. Partial-order methods for model checking: from linear time to branching time. In *11th IEEE Symposium on Logic in Computer Science (LICS)*, page 294. IEEE Computer Society Press, 1996.
- [423] G. WINSKEL. Event structures. In *Petri Nets: Central Models and Their Properties, Advances in Petri Nets*, volume 255 of *Lecture Notes in Computer Science*, pages 325–392. Springer-Verlag, 1986.
- [424] P. WOLPER. Specification and synthesis of communicating processes using an extended temporal logic. In *9th Symposium on Principles of Programming Languages (POPL)*, pages 20–33. ACM Press, 1982.
- [425] P. WOLPER. Temporal logic can be more expressive. *Information and Control*, **56**(1–2):72–99, 1983.
- [426] P. WOLPER. An introduction to model checking. Position statement for panel discussion at the Software Quality workshop, 1995.
- [427] W. YI. CCS + time = an interleaving model for real-time systems. In *18th International Colloquium on Automata, Languages and Programming (ICALP)*, volume 510 of *Lecture Notes in Computer Science*, pages 217–228. Springer-Verlag, 1991.
- [428] M. YOELI. *Formal Verification of Hardware Design*. IEEE Computer Society Press, 1990.
- [429] S. YOVINE. KRONOS: A verification tool for real-time systems. *International Journal on Software Tools for Technology Transfer*, **1**(1-2):123–133, 1997.
- [430] S. YOVINE. Model checking timed automata. In G. Rozenberg and F. Vaandrager, editors, *Lectures on Embedded Systems*, volume 1494 of *Lecture Notes in Computer Science*, pages 114–152. Springer-Verlag, 1998.

# Index

## A

absorbing state, 753, 769  
absorption law, 248, 918  
abstract  
    syntax, 916  
    transition system, **500**  
abstraction  
    function, **499**  
accept state, 152, 174  
acceptance set, 174, 193, 274  
accepting  
    bottom strongly component, 803  
    end component, 872  
    run, 154, 174, 193, 801  
*Act* set of actions, 20  
action-based bisimulation, **465**  
action-deterministic, **24**, 597  
adjacency lists, 921  
almost surely, 756  
alphabet, 912  
alternating bit protocol, 57, 60, 545, 564,  
    838  
always, 230, 319  
ample set, 605  
anti-symmetric relation, 911  
*AP* set of atomic propositions, 20  
*AP*-determinism, **24**, 512, 582  
*AP*-partition, 478  
arbiter, 50, 259, 362, 835  
arity, 911  
assignment, 65  
    random, 837  
associativity law, 918

## atomic

clock constraint, **678**  
proposition, 20, 915  
region, 65, 74  
statement, 42, 72

## B

Büchi automaton, **174**, 229, 607, 623, 800  
backward edge, 207, 208, 213, 620, 623, 624,  
    644, 923  
bad prefix, **112**, 159, 161, 199, 797  
bakery algorithm, 461, 471  
balance equation, 831  
basis, 757  
BFS, 921  
    -based reachability, 108, 390  
binary decision diagram, 381, **395**  
    one successor  $\text{succ}_1(\cdot)$ , 395  
    ordered, 395  
    reduced, **398**  
    semantics, 396  
    shared, **408**  
    zero successor  $\text{succ}_0(\cdot)$ , 395  
binary decision tree, 385  
bisimulation, **451**, 456, 732  
    action-based, **465**  
    normed, **552**  
    on a Markov chain, 808  
    quotient  $TS/\sim$ , **459**  
    step-dependent normed, **556**  
    stutter, **536**  
    stutter with divergence, **546**  
bisimulation equivalence, 451

- $\approx^n$ , **552**
- $\approx$ , **536**
- $\approx^s$ , **556**
- $\approx^{div}$ , **546**
- $\sim$ , **451**
- $\sim_{\mathcal{M}}$ , **808**
- $\sim_{TS}$ , **456**
- $\sim$  bisimulation equivalence, **451**
- bisimulation-closed  $\sigma$ -algebra, **811**
- block, **476**
- bottom strongly connected component, **774**
- branching condition (A5), **652**
- breadth-first search, **921**
- BSCC, **774, 787**
- C**
- cardinality, **910**
- channel, **53**
  - capacity, **55**
  - $cap(\cdot)$  channel capacity, **55**
  - lossy, **837**
- Chan* set of channels, **53**
- channel system, **55, 63, 68, 79, 627, 837**
  - closed, **63**
  - open, **63**
  - transition system, **59**
- characteristic function, **386**
- circuit, **77, 82, 87, 240, 301**
- clause, **919**
- clock constraint, **678**
- clock equivalence, **713**
- $\cong$  clock equivalence, **713**
- clock region, **714**
  - unbounded, **721**
- $r_\infty$  unbounded clock region, **721**
- closed channel system, **63**
- closure
  - of formula, **276**
  - of LT property, **114**
  - transitive, reflexive, **912**
- CNF, **407, 919**
- coarser, **911**
- cofactor, **383**
  - order-consistent, **397**
- communication action, **53, 70**
- Comm* set of communication actions, **53**
- communication channel, **53, 241**
- commutativity law, **918**
- complex effect, **645**
- computation tree logic, *see* CTL
- computed table, **409, 414**
- concatenation, **913**
- concurrency, **36**
- Cond*( $\cdot$ ) set of Boolean conditions, **30**
- conjunctive normal form, **919**
- coNP, **928**
  - complete, **930**
  - hard, **930**
- consistent, **276**
- constrained reachability, **762, 777**
  - step-bounded, **767**
- control
  - cycle, **642**
  - path, **642**
- counterexample, **8, 168, 199, 271, 374, 786**
- CTL
  - equivalence, **468**
  - existential fragment, **520**
  - fairness assumption, **359**
  - path formula, **317**
  - semantics, **320, 360**
  - state formula, **317**
  - syntax, **317**
  - universal fragment, **516**
- CTL\*
  - equivalence, **468**
  - existential fragment, **520**
  - semantics, **423**
  - syntax, **422**
  - universal fragment, **516**
- CTL<sup>+</sup>, **426**
- cumulative reward, **817**
- cycle, **921**



breaking condition (S2), 635  
 condition (A4), 610, 620  
 cylinder set, 757

**D**

DBA, **188**, 799  
 de Morgan's law, 918  
 deadlock, 89  
 decrementing effect, 644  
 dependence of actions, 599  
 dependency condition (A2), 609, 628  
 depth-first search, 921  
   nested, 203, 623  
 deterministic  
   algorithm, 926  
   Büchi automaton, **188**, 799  
   finite automaton, 156, 797  
   Rabin automaton, 801, 881  
   transition system, 24  
 DFA, 156  
 DFS, 921  
 digraph, 920  
 Dijkstra's dining philosophers, 90  
 dining philosophers, 90, 234, 839  
 discrete-time Markov chain, 753  
 disjoint union  $\uplus$ , 910  
 disjunctive normal form, 919  
 distribution, 755  
 distributive law, 249, 918  
 divergence  
   -sensitive expansion  $\overline{TS}$ , **575**  
   sensitivity, **544**  
   stutter bisimulation, 546  
 divergent state, **544**  
 DNF, 407, 919  
 $dom(\cdot)$  domain of message, 55  
 double negation, 918  
 DRA, 801  
   accepting run, **801**  
   language, **801**  
   run, **801**

drain, 395  
 duality rules, 248, 329  
 dynamic leader election, 242

**E**

edge, 920  
 effect, 644  
   complex, 645  
   decrementing, 644  
   incrementing, 644  
   of an action, 32  
 $Effect(\cdot)$ , 32  
 elementary sets, **276**  
 elimination rule, 400  
 emptiness problem, 155, 184, 296  
 empty word  $\varepsilon$ , 913  
 end component, **870**  
   accepting, 872  
   graph, 870  
   maximal, 875  
 ENF, 332  
 equivalence  
   class, 911  
   of NBA, **185**  
   of NFA, **155**  
   relation, 911  
 equivalence  $\equiv$   
   of CTL formulae, 329  
   of CTL\* formulae, 425  
   of CTL- and LTL formulae, 334  
   of LTL formulae, 248  
   propositional logic, 917  
 equivalence checking  
   bisimulation equivalence, 493  
   finite trace equivalence, 494  
   simulation equivalence, 528  
   stutter-bisimilarity, 567  
     with divergence, 574  
   trace equivalence, 494  
 essential variable, 383  
 evaluation, 27, 30, 382, 916

- Eval*( $\cdot$ ) variable evaluation, 27, 30, 382, 916  
 event, 754  
     measurable, 755  
 $\mathcal{E}$  set of events, 754  
 eventually, 121, 230, 318  
 execution, **25**  
 execution fragment, **24**  
 existential fragment, **520**  
 existential normal form, 332  
     CTL, **332**  
 existential quantification, 317, 418, 909  
 exit states, **571**  
*Bottom*( $\cdot$ ) set of exit states, **571**  
 expansion law  
     CTL, 329  
     LTL, 248, 249, 275  
     CTL, 330  
     PCTL, 764  
 expected  
     long-run reward, 830  
     reward, 818  
*exp*( $n$ ) exponential complexity, 910  
 expressiveness, 337
- F**
- fair  
     satisfaction relation, **135**, 259, 363, 892  
     scheduler, 884  
*FairPaths*( $\cdot$ ) set of fair paths, 134, 259, 360  
 fair satisfaction relation  $\models$   
     CTL, **360**  
     LTL, 259  
 fair satisfaction relation  $\models$   
     CTL, 361  
     LT property, 135  
     LTL, 358  
     PCTL, 891  
*FairTraces*( $\cdot$ ) set of fair traces, 134, 259  
 fairness, 126, 258, 359, 732, 883  
 fairness assumption, **133**  
     CTL, **359**  
     CTL\*, 425  
     LTL, **258**  
     MDP, 883  
     realizable, **139**, 793, 884  
 fairness constraint, 129  
     LTL, **258**  
     strong, 130, 258, 359  
     unconditional, 130, 258, 359  
     weak, 130, 258, 359  
 father, 924  
 final state, 152, 174  
*find\_or\_add*, 409  
 finer, 911  
 finite trace  
     equivalence, 117, 494  
     inclusion, 116  
 finite transition system, 20  
 finite word, 912  
 finite-memory scheduler, **848**  
 finitely branching, 472, 924  
*first*( $\cdot$ ), 95  
 fm-scheduler, 848  
 forming path, 655  
*frac*( $\cdot$ ) fractional part of real, 709  
 fully expanded, 613
- G**
- garbage collection, 265  
 generalized NBA, **193**, 274  
 global cycle, 644  
 GNBA, **193**, 274, 278  
     accepting run, **193**  
     language, **193**, 274  
     run, **193**  
 graph, 920  
     end component, 870  
     of a Markov chain, 748  
     of a transition system, **95**  
     of an MDP, 840  
     program, 30  
 guard, 33, 65

guarded command language, 63, 837  
 guess-and-check, 926

**H**

Hamiltonian path problem, 288, 356  
   vet, 924  
 handshaking, 47, **48**, 56, 466, 599, 683  
*H* set of handshaking actions, 48, 683  
 hardware circuits, 26  
 hardware verification, 5

**I**

idempotency rules, 248, 329, 918  
 iff, 909  
 image-finite, 119  
 implementation relation, 449  
   weak, 529  
 incrementing effect, 644  
 independence of actions, 37, 599  
 index of an equivalence, 911  
 $\text{inf}(\pi)$ , 749  
 infinite word, 100, 170, 912  
 initial  
   execution fragment, 25  
   path fragment, **96**  
 initial distribution  $\iota_{\text{init}}$ , 748  
 initial state, 20  
 inner node, 395  
 integral part  $[d]$  of real  $d$ , 709  
 interleaving, **36**, **38**, 40, 49  
 invariant, **107**  
   condition, 107  
 isomorphism rule, 400, 409  
 ITE, 410  
 iterated cofactor, 383

**K**

Kleene star, 913  
 Knuth and Yao's die simulation, 750  
 Knuth's die simulation, 819, 821, 838

**L**

labeling function, **20**  
 language  
   of a regular expression, 914  
   of an  $\omega$ -regular expression, 171  
   of DRA, 801  
   of GNBA, 193, 274  
   of LT property, 100  
   of NBA, 174  
   of NFA, **154**  
 language  $\mathcal{L}$ , 170, 913  
 language equivalence  
   GNBA, 193  
   NBA, 185  
   NFA, 155  
 leader election, 87, 242, 846  
 leaf, 924  
 length  
   of a formula, 916  
   of a word, 913  
 letter, 912  
 light switch, 688, 692–694, 699, 714, 727  
 limit, 871  
 limit LT property, 872, 887  
 linear temporal logic, *see* LTL  
 linear-time property, *see* LT property  
 literal, 919  
 liveness property, **121**  
 locally consistent, 276  
 location, **32**, 678  
   diagram, 682  
*Loc* set of locations, 32, 678  
 long-run reward, 830  
 LT property, **100**, 456, 796  
    $\omega$ -regular, 172, 796  
   limit, 872  
   satisfaction, **100**  
   stutter-insensitive, **535**  
 LTL  
   elementary sets, **276**  
   equivalence, 468

- fairness assumption, **258**
  - semantics, **235**, 237
  - syntax, **231**
- LTL $\setminus$ O, **534**
- M**
- Markov chain, **747**
- Markov decision process, **833**
- Markov reward model, **817**
- master formula, 471, 562, 815
- maximal
  - end component, 875
  - execution fragment, 25
  - path fragment, **96**
  - set of formulae, 276
- maximal proper state subformula, 427
- MDP, 833
- measurable event, 755
- memoryless scheduler, **847**
- message passing, 47, 56
- minimal bad prefix, **112**, 161
- mode, 848
- model checking, **11**
  - process, 11
  - strengths and weaknesses, 14
- Modify*( $\cdot$ ) set of modified variables, 627
- modified variable, 627
- modulo-4 counter, 240
- monotonic, 647
- MRM, 817
- mutex-property, 102
- mutual exclusion, 43, 45, 50, 98, 102, 161, 173, 259, 542
  - semaphore, 73
- N**
- nanoPromela, 64, 837
- IN natural numbers, 909
- NBA, **174**
  - accepting run, **174**
  - language, **174**
  - nonblocking, **187**
  - run, **174**
  - union operator, 179
- negative cofactor, 383
- nested depth-first search, 203, 623
- nesting depth, 792
- neutral, 645
- NFA, **151**
  - accepting run, **154**
  - language, **154**
  - run, **153**
- non-zeno, 694
- nonblocking
  - GNBA, 195
  - NBA, 187
- nondeterminism, 22
- nondeterministic
  - algorithm, 926
  - Büchi automaton, **174**
  - finite automaton, **151**
- nonemptiness
  - condition (A1), 609
  - problem, 155, 184
- norm function, 552
- normal form
  - existential, 332
  - positive, 252, 333, 902
- normed bisimulation, **552**, 654
- NP, 928
  - complete, 929
  - hard, 929
- O**
- $\mathcal{O}(\exp(n))$ , 910
- $\mathcal{O}(\text{poly}(n))$ , 910
- OBDD, 392
  - reduced, **398**
- observational equivalence, 589
- $\omega$ -regular
  - expression, **171**
  - language, **172**

- property, 172, 272, 796, 799
- open channel system, 63
- operational semantics, 68
- opposite actions, 647
- ordered binary decision diagram, **395**
- outcome, 754
- Outc* set of outcomes, 754
- P**
- P (complexity class), 927
- partition, **476**, 912
- path, 96
  - lifting, 454, 504, 549
  - existential quantification, 317
  - fair, 134
  - formula, 422, 698
  - fragment, **95**
  - in a digraph, 920
  - in a Markov chain, 749
  - in transition system, **96**
  - limit, 871
  - quantifier, 314, 330
  - universal quantification, 317
- Paths*( $\cdot$ ) set of paths, 96
- Paths<sub>fn</sub>*( $\cdot$ ) set of finite paths, 96
- PCTL, 780, 806, 866, 883
  - semantics, 783
- PCTL\*, 806, 883
- persistence condition, 199
- persistence property, **199**, 623, 795, 876
- Peterson's algorithm, 45, 67, 84, 161, 538, 667
- PG<sub>*i*</sub>-projection, 643
- PNF, 252, **255**, 257, 333, 902, 919
- poly-time algorithm, 927
- poly(*n*) polynomial complexity, 910
- polynomial time-bounded, 927
- positive cofactor, 383
- positive normal form, 252, 516, 902
  - CTL, **333**
  - LTL, **255**, 257
- PCTL, 902
  - propositional logic, 919
  - release, 257
  - weak until, 255
- Post*(*s*), 23, 753, 835, 920
- power method, 764
- powerset, 910
  - construction, 157
- Pre*(*s*), 23, 753, 835, 920
- pref(*P*), 115
- prefix, 913
  - of a path fragment, 96
- pref*( $\cdot$ ), **114**
- preorder, 498, 912
- probabilistic choice, 837
- probabilistic computation tree logic, *see* PCTL
- probabilistic CTL, *see* PCTL
- probability measure, 754
- probability space, 755
- Probmela, 837
- process fairness, 126
- producer-consumer system, 565
- product automaton, **156**
- product transition system, **165**, 200, 623
- program
  - nanoPromela, 64
- program graph, **32**, 34, 55, 68, 77
  - independence of actions, 599
  - interleaving, 40
  - partial order reduction, 627
  - static partial order reduction, 635
  - transition system, **34**
- projection, 643
  - function, 383
- Promela, 63, 837
- proper refinement, 911
- propositional
  - logic, 915
  - symbol, 915
- PSPACE, 928
  - complete, 930
  - hard, 930

PTIME, 927

## Q

qualitative

fragment of PCTL, **788**

property, 746

quantifier, 909

path-, 314

quantitative property, 746

quotient

transition system, 521

space, 458, 911

transition system  $TS/\approx$ , **541**

transition system  $TS/\approx^{div}$ , 546

transition system  $TS/\sim$ , **459**

transition system  $TS/\simeq$ , **508**

## R

Rabin automaton, 801

railroad crossing, 51, 683, 700

random assignment, 837

randomized

dining philosopher, 839

leader election, 846

scheduler, 850

reachability probability, 759

reachable states, **26**

$\mathbb{R}$  real numbers, 909

real-time, 246, 673

realizable, 884

reduced OBDD, **398**

reduced state space  $\hat{S}$ , 606

reduced transition relation  $\Rightarrow$ , 606

reduction rules, 400

refinement, 911

reflexive relation, 911

region, 714

reset operator, 719

region transition system, 709, 726

regular

expression, 171, 914

language, 172, **914**

property, 172

safety property, **159**, 797

relational product, 416, 419

release operator, 256, 902

R release operator, 256

release PNF, 257

rename operator, 386, 416

repeated eventually, 121

repetition

finite, 913

infinite, 171

reward function, 817

ROBDD, **398**

ROBDD-size, 400

root, 395, 924

rule for double negation, 918

run

in DRA, 801

in GNBA, 193

in NBA, 174

in NFA, 153

## S

safety property, **112**, 116, 117, 140, 159, 177, 797, 886

SAT problem, 925

Sat( $\Phi$ ), 423

satisfaction relation  $\models$

CTL, 320

CTL\*, 423

fair CTL, **360**

LT property, 100

PCTL, 783

satisfaction relation  $\models$

CTL, 321

CTL\*, 423

LTL, 235, 237

PCTL, 782, 866

propositional logic, 916

TCTL, 701

- satisfaction set, 321, 343, 423, 703  
   fair, 361
- satisfiability, 296, 918, 925
- SCC, 774, 924
- scheduler, 842  
   fair, 884  
   finite-memory, **848**  
   memoryless, **847**  
   randomized, 850  
   simple, 847
- self-loop, 920
- semantic equivalence  $\equiv$   
   propositional logic, 917
- semaphore, 43, 73, 98, 537, 542, 600, 663
- set of  
   actions, 20  
   atomic propositions, 20  
   bad prefixes, 112, 161  
   minimal bad prefixes, 112, 161  
   natural numbers  $\mathbb{N}$ , 909  
   predecessor states, 23  
   real numbers  $\mathbb{R}$ , 909  
   successor states, 23
- Shannon expansion, **384**, 397
- $\overline{\mathfrak{B}}$  shared OBDD, 408
- shared OBDD, **408**
- shared variable, 39
- $\Sigma$  alphabet, 912
- $\sigma$ -algebra, 754  
   bisimulation-closed, **811**
- $\sigma$ -algebra, 758
- simple scheduler, 847
- simulation, **497**, 506  
   equivalence, 506  
   equivalence  $\simeq$ , **505**  
    $\preceq$  simulation order, **497**  
   order  $\preceq$ , 506  
   quotient system, 508
- $\simeq$  simulation equivalence, 505
- simulator set, 506
- size  
   of an MDP, 840  
   of an OBDD, 395  
   of an ROBDD, 400
- skip, 65
- software verification, 3
- son, 924
- splitter, **483**, 568
- stability, 483
- stable, 568
- stack, 923
- standard triple, 415
- starvation freedom, 103, 121, 127, 173
- state formula, 422, 698
- state graph, **95**
- $G(TS)$  state graph of  $TS$ , 95
- state region, 714
- state space explosion, 77, 381
- statement  
   skip, 65  
   atomic $\{\dots\}$ , 66  
   nanoPromela, 65  
   exit, 68  
   sub, 69
- static partial order reduction, 635
- step-bounded  
   constrained reachability, 767  
   until, 781
- step-dependent normed bisimulation  $\approx^s$ , **556**
- sticky  
   action, 635  
   condition (A3/4), 636
- strong cycle condition (A4'), 620
- strong fairness, **130**, 259, 359, 772
- strongly connected, 774
- strongly connected component, 774, 924  
   bottom, 774
- structural induction, 281
- structured operational semantics, 34, 70
- stutter  
   action, 603  
   bisimulation  
      $\approx$ , **536**  
   bisimulation with divergence, **546**

- condition (A3), 610
  - equivalence, **530**
  - equivalence with divergence  $\approx^{div}$ , 549
  - implementation relation, 540
  - insensitive, **535**
  - step, **530**, 603
  - trace equivalence, **532**, 606
  - trace inclusion, **532**
  - $\triangleq$  stutter trace equivalence, **532**
  - $\trianglelefteq$  stutter trace inclusion, **532**
  - sub-MDP, 870
  - sub-OBDD, 396
  - subset construction, 157
  - substatement, **69**
  - subword, 913
  - $succ_b(v)$ , 395
  - success set, 873
  - successor function, 395
  - successor region, 723
  - $succ(\cdot)$  successor region, 723
  - suffix, 913
    - of a path fragment, 96
  - superblock, **476**
  - switching function, 383
  - symbol, 912
  - symbolic, 381
  - symmetric function, 406
  - symmetric relation, 911
  - synchronous product  $\otimes$ , 75, 156
- T**
- tautology, 918
  - TCTL, 698
    - model checking, 705
    - semantics, 701
    - syntax, 698
  - terminal
    - node, 395
    - state, **23**, 89
  - test-and-set semantics, 66, 72
  - time divergence, 700
  - time-convergent, 692
  - time-divergent, 692
  - timed automaton, **678**
  - timed computation tree logic, *see* TCTL
  - timed CTL
    - see* TCTL, 698
  - timelock, 692, 705, 731
  - total DBA, 188
  - total DFA, 156
  - trace, **98**
    - fair, 134
  - trace equivalence, **105**, 106, 514
    - checking, 494
  - trace fragment, **98**
  - trace inclusion, 104
    - finite, 116
  - $Traces(\cdot)$  set of traces, 98
  - $Traces_{fn}(\cdot)$  set of finite traces, 98
  - transient state distribution, 768, 828
  - transient state probabilities, 768
  - transition probability function, 748, 834
  - transition probability matrix
    - Markov chain, 748
    - Markov decision process, 834
  - transition relation  $\rightarrow$ , 20
  - transition system, **20**
    - graph, **95**
    - image-finite, 119
    - interleaving, 38
    - of a channel system, **59**
    - of a program graph, **34**
    - of a timed automaton, **687**
    - of hardware circuit, **28**
  - transitive relation, 911
  - transitive, reflexive closure, 912
  - tree, 924
  - two-step-semantics, 72
- U**
- unconditional fairness, **130**, 259, 359
  - unique table, 409



universal fragment, **516**  
universal quantification, 317, 909

## V

$\text{val}(v)$ , 395  
validity, 296, 918  
validity problem, 930  
value function, 395  
value iteration, 854, 861  
variable  
    nanoPromela, 64  
    essential, 383  
    labeling function, 395  
    ordering  $\wp$ , 395  
    ordering problem, 403  
    typed, 30  
 $\text{Var}$  set of variables, 30  
 $\text{Var}(\cdot)$  variables in an expression, 627  
variable labeling function  $\text{var}(v)$ , 395  
vertex, 920  
 $\text{Vis}$ , 635  
visibility condition (S1), 635  
visible action, 635

## W

weak fairness, **130**, 259, 359  
weak implementation relation, 529  
weak until, 252, 318, 327, 902  
 $W$  weak until, 252  
weak-until PNF, 255  
witness, 374, 786  
word, 97, 912  
    empty, 913  
    infinite, 100, 170

## Z

zeno path, 694

University of Michigan Law School  
University of Michigan Law School Scholarship Repository

---

Articles

Faculty Scholarship

---

2017

## Contracts *Ex Machina*

Kevin Werbach


*The Wharton School, University of Pennsylvania*

Nicolas Cornell

*University of Michigan Law School, [cornelln@umich.edu](mailto:cornelln@umich.edu)*

Available at: <https://repository.law.umich.edu/articles/1936>

Follow this and additional works at: <https://repository.law.umich.edu/articles>

 Part of the [Contracts Commons](#), and the [Science and Technology Law Commons](#)

---

### Recommended Citation

Cornell, Nicolas, co-author. "Contracts *Ex Machina*." K. D. Werbach, co-author. *Duke L. J.* 67 (2017): 313-82.

This Article is brought to you for free and open access by the Faculty Scholarship at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in Articles by an authorized administrator of University of Michigan Law School Scholarship Repository. For more information, please contact [mlaw.repository@umich.edu](mailto:mlaw.repository@umich.edu).

# CONTRACTS EX MACHINA

KEVIN WERBACH† & NICOLAS CORNELL††

## ABSTRACT

*Smart contracts are self-executing digital transactions using decentralized cryptographic mechanisms for enforcement. They were theorized more than twenty years ago, but the recent development of Bitcoin and blockchain technologies has rekindled excitement about their potential among technologists and industry. Startup companies and major enterprises alike are now developing smart contract solutions for an array of markets, purporting to offer a digital bypass around traditional contract law. For legal scholars, smart contracts pose a significant question: Do smart contracts offer a superior solution to the problems that contract law addresses? In this article, we aim to understand both the potential and the limitations of smart contracts. We conclude that smart contracts offer novel possibilities, may significantly alter the commercial world, and will demand new legal responses. But smart contracts will not displace contract law. Understanding why not brings into focus the essential role of contract law as a remedial institution. In this way, smart contracts actually illuminate the role of contract law more than they obviate it.*

## TABLE OF CONTENTS

Introduction .....	314
I. Contracts Get Smart.....	319
A. The Evolution of Digital Agreements .....	320
B. Bitcoin and the Blockchain .....	324
C. Blockchain-Based Smart Contracts .....	330
II. Conceptualizing Smart Contracts.....	338
A. Are Smart Contracts Contracts? .....	338
B. What's New Here? .....	343
1. <i>Smart Contracts as Escrow</i> .....	344
2. <i>Smart Contracts as Self-Help</i> .....	346
3. <i>Smart Contracts as Entire Agreements</i> .....	348

---

Copyright © 2017 Kevin Werbach & Nicolas Cornell.

† Associate Professor, Legal Studies and Business Ethics Department, The Wharton School, University of Pennsylvania.

†† Assistant Professor, University of Michigan Law School.

III. What They Teach Us About Contract Law.....	352
A. Contract Law as Enforcing Promises.....	354
B. Contract Law as Voluntary Liability .....	358
C. Contract Law as Ex Post Adjudication .....	360
IV. Smart Contracts in Practice .....	363
A. Imperfections of Algorithmic Enforcement.....	365
B. Doctrinal Concerns .....	367
1. <i>Problems with Meeting of the Minds</i> .....	368
2. <i>Problems with Consideration</i> .....	370
3. <i>Problems with Capacity</i> .....	371
4. <i>Problems with Legality</i> .....	372
C. Looking Forward.....	374
1. <i>Best Practices</i> .....	374
2. <i>Restitution</i> .....	376
3. <i>Regulation</i> .....	377
Conclusion.....	381

## INTRODUCTION

Technological advancements hold the potential to alter our very conception of the law. It is already common to suggest that technologies can operate as a kind of law, regulating the behavior of users.<sup>1</sup> But, thus far, traditional legal enforcement has generally remained available as a backstop. Is it possible for emerging technologies to displace the law even for enforcement, law’s historically essential province? In this Article, we examine a significant contemporary example, digitally enforced “smart contracts”<sup>2</sup> based on the distributed cryptocurrency technology of Bitcoin<sup>3</sup> and the

---

1. See generally LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) (arguing that “code is law”). This recognition in the legal academy of the constitutive role of technology follows a broader understanding within science and technology studies. See generally JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012) (arguing that legal and technical rules governing flows of information are out of balance); Bruno Latour, *On Technical Mediation—Philosophy, Sociology, Genealogy*, 3 COMMON KNOWLEDGE 29 (1994) (analyzing the role of technological artifacts in modern day culture).

2. A smart contract is an agreement in digital form that is self-executing and self-enforcing. See *infra* note 24 and accompanying text. The term was coined by cryptographer Nick Szabo in the 1990s. See Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, FIRST MONDAY (Sept. 1, 1997), <http://ojphi.org/ojs/index.php/fm/article/view/548/469> [<https://perma.cc/53HK-9D6W>].

3. Bitcoin is a digital currency not issued by any bank or sovereign state. Bitcoin first appeared in a paper published online in 2008 by “Satoshi Nakamoto.” See Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008) (unpublished manuscript), <https://>

blockchain that facilitates it.<sup>4</sup> Enthusiasts of various stripes believe that smart contracts offer the potential to displace the legal system's core function of enforcing agreements.<sup>5</sup>

It has traditionally been assumed that enforceable agreements—the lifeblood of the modern economic and social world—require the backing of a legal system. Nearly four centuries ago, Thomas Hobbes described the impossibility of binding agreements without the law:

If a covenant be made, wherein neither of the parties perform presently, but trust one another; in the condition of mere nature (which is a condition of war of every man against every man,) upon any reasonable suspicion, it is void: but if there be a common power set over them both, with right and force sufficient to compel performance, it is not void. For he that performeth first, has no assurance the other will perform after, because the bonds of words are too weak to bridle men's ambition, avarice, anger, and other passions, without the fear of some coercive power . . . .

But in a civil estate, where there a power set up to constrain those that would otherwise violate their faith . . . he which by the covenant is to perform first, is obliged so to do.<sup>6</sup>

Hobbes's basic idea—that binding agreements require a system to ensure that counterparties can trust one another to perform—is an

---

bitcoin.org/bitcoin.pdf [https://perma.cc/B777-M9F5]. Cryptocurrency is the more general term for currency-like tokens, like Bitcoin, that are secured through cryptography rather than traditional means.

4. A blockchain is a distributed ledger of transactions like the one created for Bitcoin. *See id.* (“We define an electronic coin as a chain of digital signatures.”). Every node in a blockchain network verifiably sees the same transaction record, even though there is no master copy. Bitcoin uses this platform for a currency, with the ledger guaranteeing that the same coin cannot be spent twice. Smart contracts use blockchains to generalize the approach to any digitally expressible transaction.

5. *See* Matt Byrne, *Do Lawyers Have a Future?*, LAW. (Sept. 20, 2016), <https://www.thelawyer.com/issues/online-september-2016/do-lawyers-have-a-future-2> [https://perma.cc/H2P4-BC94] (“Numerous futurists predict that smart contracts, using the developing technologies of blockchain and less strict coding languages, will result in contracts being written as immutable code on private blockchains, humming along harmoniously and self-executing and self-regulating.”); Alan Cunningham, *Decentralisation, Distrust & Fear of the Body—The Worrying Rise of Crypto-Law*, SCRIPTED 237 (Dec. 2016), <https://script-ed.org/wp-content/uploads/2016/12/13-3-cunningham.pdf> [https://perma.cc/PAP2-VWVA] (“It is suggested that that the use of a blockchain . . . will guarantee the enforceability element of such transactions, without any need for . . . trust in the law as a reliable social praxis.”).

6. THOMAS HOBBS, LEVIATHAN 91 (Oxford Univ. Press 1996) (1651). *See generally* Anthony T. Kronman, *Contract Law and the State of Nature*, 1 J.L. ECON. & ORG. 5 (1985) (examining the possibilities for assurance without state-imposed enforcement).

intuitive and powerful argument for the essential role of the law.<sup>7</sup>

Yet recent technological advances have led to speculation that smart contracts might largely, or entirely, displace the apparatus of contract law.<sup>8</sup> As one commentator succinctly puts this radical claim, “[s]mart contracts don’t [need] a legal system to exist: they may operate without any overarching legal framework. De facto, they represent a technological alternative to the whole legal system.”<sup>9</sup> Mainstream legal trade journals wonder whether “innovations offered by the Bitcoin 2.0 generation of technology may create a world where . . . technology renders some contract causes of action obsolete.”<sup>10</sup> Even world leaders have taken notice, like Russian Prime Minister Dmitry Medvedev, who declared that “[s]mart [c]ontracts represent [a] new challenge to legal regulation. Systems creating such contracts live by their own rules, beyond the boundaries of law.”<sup>11</sup> In short, smart contracts may offer the hope—or possibly the threat—of circumventing Hobbes’s age-old essential role for the law.

The reaction to these new possibilities runs the gamut, from gleeful triumph to killjoy skepticism. Supporters claim smart contracts

---

7. Cf. Arthur Ripstein, *Private Order and Public Justice: Kant and Rawls*, 92 VA. L. REV. 1391, 1418 (2006) (“Private enforcement is not merely inconvenient: it is inconsistent with justice because it is ultimately the rule of the stronger.”).

8. See DON TAPSCOTT & ALEX TAPSCOTT, *BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD* 47 (2016) (“Smart contracts are unprecedented methods of ensuring contractual compliance, including social contracts.”); Byrne, *supra* note 5; Cunningham, *supra* note 5, at 254; Rob Marvin, *Blockchain in 2017: The Year of Smart Contracts*, PCMAG (Dec. 12, 2016), <http://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts> [<https://perma.cc/2K96-PVVR>] (quoting Jeff Garzik, Linux Board member, as saying that smart contracts will offer “adjudication-as-a-service,” which will be “a hyper real-time version of the court system”).

9. Alexander Savelyev, *Contract Law 2.0: «Smart» Contracts as the Beginning of the End of Classic Contract Law* 21 (Nat’l Research Univ. Higher Sch. of Econ., Working Paper No. BRP 71/LAW/2016, 2016), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2885241](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241) [<https://perma.cc/HS7F-PF3W>].

10. Andrew Hinkes, *Blockchains, Smart Contracts, and the Death of Specific Performance*, INSIDE COUNSEL (July 29, 2014), <http://www.insidecounsel.com/2014/07/29/blockchains-smart-contracts-and-the-death-of-speci> [<https://perma.cc/6FSQ-TT47>]; see also Byrne, *supra* note 5 (“Numerous futurist predict that smart contracts, using the developing technologies of blockchain and less strict coding languages will result in contracts being written as immutable code on private blockchains, humming along harmoniously and self-executing and self-regulating. All of a sudden, the disruption we have seen in other sectors is knocking at our own doors. But, we need not panic. At least, not yet.”).

11. Savelyev, *supra* note 9, at 15 (citing Dmitry Medvedev, *Vystupleniye Dmitriya Medvedeva na plenarnom zasedanii* [Speech of Dmitry Medvedev on Plenary Session], Saint Petersburg International Legal Forum (May 18, 2016)).

will obviate the need for contract law, revolutionize business arrangements, and restructure property ownership.<sup>12</sup> Skeptics see the blockchain foundation as little more than a Ponzi scheme.<sup>13</sup> Some technologists argue that, despite their name, smart contracts have nothing to do with contracts.<sup>14</sup> One group conspicuously absent from the debate over smart contracts is contract law scholars.

Upon inspection, the story is complex. Smart contracts may or may not transform the world, but they provide real benefits and seem likely to enjoy significant adoption over time. They represent the mature end of the evolution of electronic agreements over several decades.<sup>15</sup> Firms can achieve significant cost savings and efficiency gains when using computers to automate contracting.<sup>16</sup> Smart contracts

---

12. See, e.g., ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES 2 (2016) (“Optimists claim that Bitcoin will fundamentally alter payments, economics, and even politics around the world.”); NORTON ROSE FULBRIGHT LLP, CAN SMART CONTRACTS BE LEGALLY BINDING CONTRACTS? 2 (2016), <http://www.nortonrosefulbright.com/knowledge/publications/144559/can-smart-contracts-be-legally-binding-contracts> [<https://perma.cc/SKV7-Z8P8>] (quoting R3 consortium CEO David Rutter stating that “smart contracts . . . will set the scene for the next twenty years of finance”); *Not-So-Clever Contracts*, ECONOMIST (July 30, 2016), <https://www.economist.com/news/business/21702758-time-being-least-human-judgment-still-better-bet-cold-hearted> [<https://perma.cc/E6WR-TKLH>] (“Such ‘smart contracts’ are all the rage among futurist backers of the blockchain, the technology that underpins bitcoin, a digital currency.”).

13. A Ponzi scheme is a form of investment fraud in which earlier investors are paid returns out of funds contributed by new investors, rather than from actual profits. See *Fast Answers: Ponzi Schemes*, U.S. SEC. & EXCHANGE COMMISSION (Oct. 9, 2013), <https://www.sec.gov/fast-answers/answersponzihtm.html> [<https://perma.cc/BFB6-4T8C>]. Critics argue that the value of Bitcoin depends on a steady stream of new purchasers willing to buy the digital currency at higher prices, even though earlier purchasers (seeking investment returns) do not actually use it to buy anything, eventually causing a collapse. See Matt O’Brien, *Bitcoin Isn’t the Future of Money—It’s Either a Ponzi Scheme or a Pyramid Scheme*, WASH. POST: WONKBLOG (June 8, 2015), <http://www.washingtonpost.com/blogs/wonkblog/wp/2015/06/08/bitcoin-isnt-the-future-of-money-its-either-a-ponzi-scheme-or-a-pyramid-scheme/> [<https://perma.cc/7BRH-Y7VE>]; Eric Posner, *Fool’s Gold*, SLATE (Apr. 11, 2013, 11:11 AM) [http://www.slate.com/articles/news\\_and\\_politics/view\\_from\\_chicago/2013/04/bitcoin\\_is\\_a\\_ponzi\\_scheme\\_the\\_internet\\_currency\\_will\\_collapse.html](http://www.slate.com/articles/news_and_politics/view_from_chicago/2013/04/bitcoin_is_a_ponzi_scheme_the_internet_currency_will_collapse.html) [<https://perma.cc/NQ8R-77ZB>]; see also Ferdinando Ametrano, *Why 2017 Will Prove ‘Blockchain’ Was a Bad Idea*, COINDESK (Jan. 4, 2017), <http://www.coindesk.com/2017-will-prove-blockchain-bad-idea> [<https://perma.cc/4HCX-PGX9>] (“Probably some smart contract hype will clutter the debate, thanks to the smartest ones among the fools trying to outsmart even the smart contract inventor.”).

14. See, e.g., *Explainer: Smart Contracts*, MONAX, [https://monax.io/explainers/smart\\_contracts](https://monax.io/explainers/smart_contracts) [<https://perma.cc/45AT-KUEF>] (“To begin with, smart contracts are neither particularly smart nor are they, strictly speaking, contracts.”).

15. See generally Harry Surden, *Computable Contracts*, 46 U.C. DAVIS L. REV. 629 (2012) (describing the development of data-oriented and computable digital contracts).

16. See, e.g., JAMES SCHNEIDER ET AL., GOLDMAN SACHS, BLOCKCHAIN: PUTTING THEORY INTO PRACTICE (2016), <https://www.scribd.com/doc/313839001/Profiles-in-Innovation->

could greatly extend those benefits, by taking advantage of Bitcoin and the blockchain as open platforms for secure exchange of value without mutual trust.<sup>17</sup> As they are adopted, or used in lieu of traditional contracting, smart contracts will force courts, legislatures, and other legal actors to confront difficult questions about the application of basic contract doctrines.

They will not, however, replace contract law. While smart contracts can meet the doctrinal requirements of contract law,<sup>18</sup> they serve a fundamentally different purpose. Contract law is a remedial institution. Its aim is not to ensure performance *ex ante*, but to adjudicate the grievances that may arise *ex post*.<sup>19</sup> Smart contracts bring this core function of contract law into sharper relief, as they eliminate the act of remediation by admitting no possibility of breach.<sup>20</sup> But, the needs that gave rise to contract law do not disappear. If the parties do not or cannot represent all possible outcomes of the smart contract arrangement *ex ante*, the results may diverge from their mutual intent. The parties' expression may also not produce legally sanctioned outcomes, as in the case of duress, unconscionability, or illegality. Promise-oriented disputes and grievances will not disappear, but their complexions will shift. In such scenarios, either the parties or the state will seek to reintroduce the machinery of contractual adjudication. Once one properly appreciates what is—and what is not—the function of contract law, it becomes evident that the reports of its death are “greatly exaggerated.”<sup>21</sup>

---

May-24-2016-1<https://www.scribd.com/doc/313839001/Profiles-in-Innovation-May-24-2016-1>  
[<https://perma.cc/WP5P-JPZF>] (identifying several ways to use blockchain-based smart contracts which could save billions of dollars per year).

17. See generally Kevin Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, 32 BERKELEY TECH. L.J. (forthcoming 2018) (conceptualizing the blockchain as a new architecture for trust).

18. See *infra* Part II.A.

19. Cf. RESTATEMENT (SECOND) OF CONTRACTS ch. 16, intro. note (AM. LAW INST. 1981) (“The traditional goal of the law of contract remedies has not been compulsion of the promisor to perform his promise but compensation of the promisee for the loss resulting from breach.”); Nicolas Cornell, *A Complainant-Oriented Approach to Unconscionability and Contract Law*, 164 U. PA. L. REV. 1131, 1164 (2016) (“[C]ontract law provides a legal remedy to those who have complaints arising out of broken agreements. It is purely retrospective; it concerns the relations that occur once something impermissible is done.”).

20. See Hinkes, *supra* note 10.

21. Though now part of popular culture, the familiar turn of phrase attributed to Mark Twain appears to be a slight misquotation. Twain’s original comment was “the report of my death was an exaggeration.” SHELLEY FISHER FISHKIN, *LIGHTING OUT FOR THE TERRITORY: REFLECTIONS ON MARK TWAIN AND AMERICAN CULTURE* 134 (1996).



The remainder of this Article unfolds as follows. In Part I, we describe the history and operation of smart contracts. In Part II, we evaluate smart contracts, which have been undertheorized so far, by asking how existing legal categories might apply to smart contracts. In Part III, we consider whether smart contracts can serve as a substitute for contract law. We answer this question in the negative, by analyzing the larger question of what contract law is for. In Part IV, we consider likely responses to the practical and doctrinal questions we raise. Surprisingly for the libertarian proponents of smart contracts, they may force the expansion of public law into the private law preserve of contracts.<sup>22</sup> The only way to prevent serious negative outcomes from smart contracts may be for governments to regulate them.

### I. CONTRACTS GET SMART

The cryptographer Nick Szabo defined a smart contract as “a set of promises, specified in digital form, including protocols within which the parties perform on these promises.”<sup>23</sup> By using “a set of promises,” Szabo left open whether a smart contract was enforceable as a legal contract.<sup>24</sup> We consider this question below.<sup>25</sup> Szabo’s reference to “protocols within which” parties perform is similarly coy. Smart contracts do not just specify these protocols; they actually implement them. Szabo’s definition has not been universally adopted, and subsequent authors offer subtly varied descriptions of the term. For

---

22. See, e.g., Aaron Wright & Primavera de Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* 4 (Mar. 12, 2015) (unpublished manuscript), [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2580664](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664) [<https://perma.cc/RQR3-VJCZ>] (suggesting that “[i]f blockchain technology becomes more widely adopted, centralized authorities, such as governmental agencies and large multinational corporations, may lose the ability to control and shape the activities of disparate people through existing means”).

23. Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets*, U. AMSTERDAM (1996), [http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOT\\_winterschool2006/szabo.best.vwh.net/smart\\_contracts\\_2.html](http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOT_winterschool2006/szabo.best.vwh.net/smart_contracts_2.html) [<https://perma.cc/YC35-2MXQ>]. Max Raskin uses a simpler definition: “agreements wherein execution is automated, usually by computers.” Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305, 306 (2017); see also Josh Stark, *Making Sense of Blockchain Smart Contracts*, COINDESK (June 4, 2016, 6:39 PM), <http://www.coindesk.com/making-sense-smart-contracts> [<https://perma.cc/533S-JUAJ>] (“Many debates about the nature of smart contracts are really just contests between competing terminology.”).

24. Other authors on the topic include the word “contract” in their definitions. For example, Wright and de Filippi define smart contracts as “digital, computable contracts where the performance and enforcement of contractual conditions occur automatically, without the need for human intervention.” See Wright & de Filippi, *supra* note 22, at 10–11.

25. See *infra* Part II.A.

purposes of this Article, we define a smart contract as an agreement in digital form that is self-executing and self-enforcing.<sup>26</sup>

In this Part, we examine the history and workings of smart contracts. Smart contracts represent the fusion of two lines of technological development: electronic contracting and cryptography. Smart contracts were first theorized and named two decades ago, but significant interest in, and implementation of, smart contracts has occurred only recently. Smart contracts could represent merely the latest step the evolution of electronic agreements, or, smart contracts' use of blockchain technology could distinguish them from any of their antecedents.

### A. *The Evolution of Digital Agreements*

Thanks to their speed and power, computers have taken over many forms of human interaction over the past half century. Email and instant messages substitute for letters and phone calls, accountants use spreadsheets and enterprise resource planning software rather than paper ledgers, and travelers use online ticketing systems rather than going to a travel agent—to give just a handful of examples. This automation has had major impacts on employment, the conduct of business, and social interactions. In many cases, it has raised significant legal and policy questions. The realm of contracting has not been immune.

Contractual agreements embodied in software code, and even their automatic performance, are nothing new.<sup>27</sup> For several decades, larger corporations have used electronic data interchange (EDI) formats to communicate digitally across supply chains.<sup>28</sup> The internet brought electronic commerce (e-commerce) to ordinary consumers, who accede to a digital contract every time they begin a relationship with an online service provider by clicking a button.<sup>29</sup> Despite its digital

---

26. In addition to execution and enforcement, smart contract-related technologies could support the full range of contractual activity, including precontractual negotiation, contract formation, and postcontractual modification. See, e.g., OPENLAW, <http://openlaw.io> [<https://perma.cc/D8EZ-D5PW>] (offering tools to “[c]reate, store, and execute legal agreements that interact with blockchain-based smart contracts.”). We explain the centrality of enforcement to smart contracts below at Part I.C.

27. See Surden, *supra* note 15, at 634.

28. EDI, which has been around since the 1970s, refers generally to automated digital communications between or within firms, much of which goes beyond the bounds of contracting language. See JANE K. WINN & BENJAMIN WRIGHT, LAW OF ELECTRONIC COMMERCE § 5-09 (4th ed. 2001) (describing EDI); Surden, *supra* note 15, at 639 n.30.

29. See Brett Frischmann & Evan Selinger, *Engineering Humans with Contracts* 8 (Benjamin

costume, this sort of electronic contract is still a written agreement—while it is electronic in *form*, its substance and execution are still dependent on humans. A user who clicks the hyperlink to read the terms of service for Facebook or Amazon.com would then see a document that spells out the contractual terms. Courts apply contract law to such agreements in the same way as to a paper document. The major doctrinal question raised here is acceptance, because most consumers barely realize the existence of, let alone read, the contractual text; that said, courts have little difficulty disposing of this objection.<sup>30</sup>

The step beyond an electronic contract is what Professor Harry Surden labels a “data-oriented” contract. In these contracts, “the parties have expressed one or more terms or conditions of their agreement in a manner designed to be processable by a computer system.”<sup>31</sup> The distinction here is that the primary audience for the contract is a machine rather than a human.<sup>32</sup> For example, a financial option contract may grant the right to purchase a stock at a given price, and expire on a certain date. A data-oriented contract would represent that arrangement in computer code. A brokerage house could then, if the conditions are met, direct its computer system to transfer the security to the buyer’s account and debit the correct sum.

The next stage in Surden’s typology is a “computable” contract.<sup>33</sup> It gives the computer systems that implement data-oriented contracts the power “to make automated, *prima-facie* assessments about compliance or performance.”<sup>34</sup> In the option contract example above,

---

N. Cardozo Sch. of Law, Faculty Research Paper No. 493, 2016), [https://papers.ssrn.com/sol3/papers2.cfm?abstract\\_id=2834011](https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2834011) [<https://perma.cc/VEE3-BU99>].

30. See *Hill v. Gateway 2000, Inc.*, 105 F.3d 1147, 1149 (7th Cir. 1997); *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1452–53 (7th Cir. 1996). Courts have been willing to find the requisite evidence of acceptance lacking based on particular facts. See, e.g., *Specht v. Netscape Commc’ns Corp.*, 306 F.3d 17, 35 (2d Cir. 2002).

31. Surden, *supra* note 15, at 639.

32. In fact, the term is even more limited. See *id.* at 640 (“The data-oriented label simply suggests that the parties have decided that *some* subset of key terms or conditions would benefit from being represented as computer processable data.” (emphasis in original)).

33. Professor Lauren Henry Scholz applies a different typology of “algorithmic” contracts, defined as those “that contain terms that were determined by algorithm rather than a person.” Lauren Henry Scholz, *Algorithmic Contracts*, 20 STAN. TECH. L. REV. (forthcoming 2017) (manuscript at 12), <https://ssrn.com/abstract=2747701> [<https://perma.cc/64Z5-NNRD>]. Scholz’s focus is on formation. We believe the degree to which execution and enforcement are automated is the critical variable for thinking about smart contracts, with algorithmic formation raising its own set of issues.

34. See Surden, *supra* note 15, at 636.

the brokerage house computer system itself could evaluate whether the price and timing of a proposed purchase met the terms of the option. The requirements for a computable contract are that the semantics—the meaning of the contractual terms—can be expressed through a set of instructions or logic that a computer can process, and that any data necessary for that computation are available in digital form.<sup>35</sup> Giving machines the ability to determine whether a contract has been performed can dramatically reduce transaction costs.<sup>36</sup> Although there are significant challenges in accurately representing and interpreting contractual semantics in computer form, finance and similar fields employ computable contracts widely.<sup>37</sup>

The evolution from electronic, to data-oriented, to computable contracts embodies a trend toward greater machine autonomy. As computers can increasingly replace humans in negotiating, forming, performing, and enforcing contracts, contracts can increasingly operate with the speed and consistency of machines. Further, computable contracts can enable machines to contract automatically with one another, although such autonomous operation is still relatively limited.<sup>38</sup>

The limitation of computable contracts is that the computers involved can only make *prima facie* determinations about performance.<sup>39</sup> The legal system and other traditional mechanisms remain available to the parties if they are unsatisfied with the results of automated systems.<sup>40</sup> The contract is designed to be computable, but if the computation diverges from the parties' intent, as conventionally understood in contract law, they may disregard the computerized

---

35. *See id.* at 664.

36. *See id.* at 689–95.

37. *See id.* at 634.

38. *See id.* at 695.

39. *See id.* at 637 n.25.

40. Surden's article, which appeared in 2012, makes no reference to smart contracts or the blockchain. More recently, Flood and Goodenough show formally that financial contracts can be represented as finite-state machines, which are subject to computational interpretation. *See* Mark D. Flood & Oliver R. Goodenough, *Contract as Automaton: The Computational Representation of Financial Agreements passim* (Office of Fin. Research, Working Paper No. 15-04, 2015), <http://ssrn.com/abstract=2538224> [<https://perma.cc/9ZJF-9AT9>]. However, Flood and Goodenough similarly fail to discuss the implications of implementing these formalized agreements as smart contracts. *Id.*; *see also* Cristian Prisacariu & Gerardo Schneider, *A Formal Language for Electronic Contracts*, in *FORMAL METHODS FOR OPEN OBJECT-BASED DISTRIBUTED SYSTEMS* 174–89 (Marcello M. Bonsangue & Einar Broch Johnsen eds., 2007) (proposing a formal language for writing electronic contracts).

result.<sup>41</sup>

In 1996, Szabo began to publish a series of articles and blog posts outlining the functions and technical requirements for what he labeled “smart contracts.”<sup>42</sup> Szabo’s starting point was that “protocols, running on public networks such as the Internet, both challenge and enable us to formalize and secure new kinds of relationships in this new environment, just as contract law, business forms, and accounting controls have long formalized and secured business relationships in the paper-based world.”<sup>43</sup> He suggested that “[t]he contractual phases of search, negotiation, commitment, performance, and adjudication . . . can be embedded in [] hardware and software.”<sup>44</sup> Many of those functions were already being implemented electronically at the time, or would be soon with the rise of e-commerce.<sup>45</sup> The visionary aspect of Szabo’s concept was that hardware and software *alone* would handle the full lifecycle of contractual activity. Human action could be completely replaced in various parts of contractual exchange.

Szabo’s smart contracts did not require fancy technology. His primary example was the humble vending machine.<sup>46</sup> The simple electronic mechanism of a vending machine performs two critical functions. First, it directly effectuates performance by taking in money and dispensing products. Second, it incorporates enough security to make the cost of breach (breaking into the machine) exceed the potential rewards.<sup>47</sup> For all practical purposes, the vending machine is

---

41. In some circumstances, those harmed by failures of computerized agreements may ultimately be held responsible for their mistake. *See, e.g.,* David Z. Morris, *Computer Error Costs T. Rowe Price \$190 Million in Dell Buyout Settlement*, FORTUNE (June 4, 2016), <http://fortune.com/2016/06/04/computer-error-t-rowe-price-dell/> [<https://perma.cc/H3UZ-ZBSQ>] (noting that T. Rowe Price was not entitled to settlement proceeds because a computerized system mistakenly voted its shares in favor of an acquisition that the firm publicly opposed). In such situations, however, the aggrieved party is still entitled to its day in court.

42. *See* Szabo, *supra* note 2; Szabo, *supra* note 23; Nick Szabo, *The Idea of Smart Contracts* (1997), [http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOT\\_winterschool2006/szabo.best.vwh.net/smart\\_contracts\\_idea.html](http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOT_winterschool2006/szabo.best.vwh.net/smart_contracts_idea.html) [<https://perma.cc/XF47-62RC>]; Nicholas J. Szabo, Presentation for Keynote Address at the IEEE International Workshop on Electronic Contracting: Smart Contracts (July 6, 2004), <http://w-uh.com/download/WECSmartContracts.pdf> [<https://perma.cc/6HQU-EYR5>]. The exact introduction date of the concept is uncertain; Szabo stated that he had been refining the idea of smart contracts since “the early 1990s.” Szabo, *supra* note 2, at n.1.

43. Szabo, *supra* note 2.

44. *Id.*

45. *See* WINN & WRIGHT, *supra* note 28 (discussing EDI systems that firms have used since the 1970s to automate contractual transactions and other communications).

46. *See* Szabo, *supra* note 2.

47. *See id.*

the entire contractual environment for its transactions. It is not limited to the prima facie decisions of Surden's computable contracts, because its performance of the contract is effectively final.<sup>48</sup>

Szabo's vision, the full automation of forming and performing contracts, was ahead of its time. His work, and similar ideas by others, were recognized within the community of "cypherpunks" who design technical mechanisms to ensure security and privacy without reliance on governments.<sup>49</sup> However, these ideas remained largely isolated from the e-commerce world.<sup>50</sup>

### *B. Bitcoin and the Blockchain*

The development that made Szabo's vision of smart contracts more than a mere curiosity was Bitcoin, a digital currency not reliant on governments, banks, or other intermediary institutions.<sup>51</sup> Since it appeared in a mysterious 2008 post by the pseudonymous Satoshi Nakamoto,<sup>52</sup> Bitcoin has provoked intense interest. Less than a decade after publication of Nakamoto's paper, Bitcoin has spawned an entire ecosystem of developers, entrepreneurs, investors, traders, and analysts, working toward a vision of technologically enabled economic and social transformation.<sup>53</sup> Over one hundred thousand firms, including major companies such as Microsoft, Dell Computer, Dish Network, Time Inc., and Overstock.com, accept Bitcoin-denominated transactions,<sup>54</sup> and the nominal value of Bitcoins in circulation

---

48. If the vending machine fails to perform the contract, such as when the product becomes stuck and is not dispensed to the customer, a remedy outside the machine may be available.

49. See Nathaniel Popper, *Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin*, N.Y. TIMES (May 15, 2015), <http://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html> [https://perma.cc/G4UE-QU4L]; Benjamin Wallace, *The Rise and Fall of Bitcoin*, WIRED (Nov. 23, 2011, 2:52 PM), [https://www.wired.com/2011/11/mf\\_bitcoin/](https://www.wired.com/2011/11/mf_bitcoin/) [https://perma.cc/7XAK-A8GY].

50. See Wright & de Filippi, *supra* note 22, at 10 ("[Blockchain] technology has breathed life into a theoretical concept [of smart contracts that Szabo] first formulated in 1997.").

51. As described below in this Section, Bitcoin is technically a specific implementation of blockchain-based cryptocurrencies, or more precisely, the currency token associated with that implementation. Smart contracts, the focus of this Article, may be implemented on the Bitcoin blockchain or other blockchains.

52. See Nakamoto, *supra* note 3. The identity of the person or persons who authored the paper remains unknown. See Popper, *supra* note 49.

53. See generally NATHANIEL POPPER, *DIGITAL GOLD: BITCOIN AND THE INSIDE STORY OF THE MISFITS AND MILLIONAIRES TRYING TO REINVENT MONEY* (2015) (surveying the burgeoning Bitcoin community).

54. See *State of Bitcoin 2015: Ecosystem Grows Despite Price Decline*, COINDESK (Jan. 7, 2015), <http://www.coindesk.com/state-bitcoin-2015-ecosystem-grows-despite-price-decline> [https://perma.cc/KYV3-7S8J].

exceeded \$110 billion in early November 2017.<sup>55</sup> Venture capitalists have funded scores of Bitcoin-based startups, investing over \$1 billion so far.<sup>56</sup> Most of the world's largest financial services firms are exploring or implementing related technologies. Legal scholars are beginning to take notice as well.<sup>57</sup>

The core attribute of Bitcoin is that it allows unrelated individuals and organizations to have confidence in transactions without trusting intermediaries or a legal system.<sup>58</sup> A currency requires trust because buyers and sellers must believe that the tokens they exchange for assets of value will themselves have value. A one hundred dollar bill without the “full faith and credit” of the United States of America is just a piece of paper featuring a green portrait of Benjamin Franklin. Bitcoin supplies a mechanism of trust that does not require the backing of any trusted institution or government. And that same mechanism can be employed for other kinds of transactions.

To supply this mechanism, Bitcoin uses a technology called “distributed ledgers.”<sup>59</sup> A distributed ledger allows any number of computers to keep an identical record of information, without reference to a central master copy—indeed, no master copy exists.<sup>60</sup> This allows Bitcoin users to be confident that the same user cannot spend the same digital coin multiple times, but that turns out to be just one of many ways to use distributed ledgers. Developers and

---

55. See *Market Capitalization*, BLOCKCHAIN (2017), <https://blockchain.info/charts/market-cap> [<https://perma.cc/63GA-DENX>].

56. See Garrick Hileman, *State of Blockchain Q1 2016: Blockchain Funding Overtakes Bitcoin*, COINDESK (May 11, 2016), <http://www.coindesk.com/state-of-blockchain-q1-2016/> [<https://perma.cc/6K7J-D5S8>].

57. See generally Joshua A.T. Fairfield, *BitProperty*, 88 S. CAL. L. REV. 805 (2015) (discussing “smart property” built on the foundation of smart contracts); Raskin, *supra* note 23 (evaluating smart contracts as a form of contractual self-help); Wright & de Filippi, *supra* note 22 (considering the implications of the blockchain and smart contracts as a new kind of law).

58. Pete Rizzo, *VC Fred Wilson: Block Chain Could Be Bigger Opportunity than Bitcoin*, COINDESK (May 5, 2014), <http://www.coindesk.com/vc-fred-wilson-block-chain-bigger-opportunity-bitcoin> [<https://perma.cc/AW62-C74H>]; Rob Wile, *Satoshi's Revolution: How the Creator of Bitcoin May Have Stumbled onto Something Much, Much Bigger*, BUS. INSIDER (Apr. 22, 2014), <http://www.businessinsider.com/the-future-of-the-blockchain-2014-4> [<https://perma.cc/9KFD-4XP2>].

59. Strictly speaking, not all distributed ledgers aggregate transactions into chains of blocks. However, “the blockchain” is commonly used to describe all similar systems.

60. See Hal Hodson, *Bitcoin Moves Beyond Mere Money*, NEW SCIENTIST (Nov. 20, 2013), <http://www.newscientist.com/article/dn24620-bitcoin-moves-beyond-mere-money.html#.VZmDmqa-uf4> [<https://perma.cc/MUX8-S7M2>]; *Blockchain: The Next Big Thing—Or Is It?*, ECONOMIST (May 9, 2015), <http://www.economist.com/news/special-report/21650295-or-it-next-big-thing> [<https://perma.cc/JZ29-CTF5>].

entrepreneurs are actively working on applying this technology to cloud file storage,<sup>61</sup> ridesharing,<sup>62</sup> name registration (as for the internet's Domain Name System),<sup>63</sup> crowdfunding,<sup>64</sup> device management for the Internet of Things,<sup>65</sup> online voting,<sup>66</sup> verification of ownership and time-stamping for digital documents,<sup>67</sup> prediction markets,<sup>68</sup> and even establishing the provenance of wine.<sup>69</sup>

There are three primary elements to the Bitcoin architecture: the ledger, the network, and consensus. These three elements combine to create a mechanism for ensuring trustworthiness without requiring trust in any particular institution or agent.<sup>70</sup> That means users can have confidence that a transaction on the network is legitimate, accurate, and not duplicated.

The first element, the distributed ledger of transactions, is commonly called the blockchain.<sup>71</sup> This database grows as it steadily incorporates new approved transactions. A Bitcoin transaction is a cryptographically signed<sup>72</sup> statement on the blockchain transferring

61. See, e.g., MAIDSAFE, <http://maidsafe.net> [<https://perma.cc/VYK3-GZ6L>]; STORJ, <http://storj.io/> [<https://perma.cc/AT8D-68UM>].

62. See Amanda Johnson, *La'Zooz: The Decentralized Proof-of-Movement "Uber" Unveiled*, COINTELEGRAPH (Oct. 19, 2014), <http://cointelegraph.com/news/112758/lazooz-the-decentralized-proof-of-movement-uber-unveiled> [<https://perma.cc/8HRX-DUYP>].

63. See, e.g., NAMECOIN, <https://namecoin.info> [<https://perma.cc/SE6M-AEAX>].

64. See, e.g., BLOCKTRUST, <https://blocktrust.org> [<https://perma.cc/5NGX-HMWS>].

65. See Paul Brody & Veena Pureswaran, *Device Democracy: Saving the Future of the Internet of Things*, IBM *passim* (2015), <http://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF> [<https://perma.cc/XC4G-3ZFF>].

66. See Danny Bradbury, *How Block Chain Technology Could Usher in Digital Democracy*, COINDESK (June 16, 2014, 11:05 PM), <http://www.coindesk.com/block-chain-technology-digital-democracy> [<https://perma.cc/X4RL-CTJM>].

67. *What is Proof of Existence?*, PROOF OF EXISTENCE, <http://www.proofofexistence.com/about> [<https://perma.cc/ZF9Q-TWUZ>].

68. Jack Peterson & Joseph Krug, *Augur: A Decentralized, Open-Source Platform for Prediction Markets passim* (2015) (unpublished manuscript), <https://bravenewcoin.com/assets/Whitepapers/Augur-A-Decentralized-Open-Source-Platform-for-Prediction-Markets.pdf> [<https://perma.cc/XV6G-GM3W>].

69. *The Future of Wine Provenance Is Bitcoin*, VINFOLIO BLOG (Oct. 6, 2014), <http://blog.vinfo.com/2014/10/06/the-future-of-wine-provenance-is-bitcoin> [<https://perma.cc/W4BX-82P7>].

70. See generally Werbach, *supra* note 17 (describing the "trustless trust" architecture).

71. See Fairfield, *supra* note 57, at 808.

72. A cryptographic signature is a secure means of verifying authenticity. It verifies that the transaction was authorized by the possessor of a private key, without actually distributing the key. With this approach, Bitcoin transactions can be quasi-anonymous. They are associated with a particular account, so it is often possible to correlate multiple transactions with the same account holder, but no identifying information about the account holder needs to be provided on the



Bitcoin tokens between two or more cryptographic private keys. These transactions are grouped together into blocks, with a new block appended approximately every ten minutes.<sup>73</sup> Every block contains an abbreviated reference, called a cryptographic hash, to the block before it, which keeps the blocks in the proper order. Anyone can view a Bitcoin's blockchain, and trace back transactions all the way to the original "genesis block" created by Nakamoto.<sup>74</sup> In theory, no one can alter an existing transaction, because every block is linked in an immutable sequence.<sup>75</sup>

The second element is the network. The blockchain is not stored in one central location.<sup>76</sup> Instead, computer nodes running the Bitcoin software connect in a peer-to-peer (P2P) network, where each maintains a complete copy of the blockchain. Every transaction is broadcast across the network to all nodes, which then add valid blocks to the blockchain on a regular basis.<sup>77</sup> Individual consumers do not need to operate a full node; they can use third-party wallet services to host their Bitcoins and connect to a service provider on the Bitcoin network.<sup>78</sup>

The final element, consensus, is perhaps the least intuitive aspect of Bitcoin,<sup>79</sup> but perhaps its most significant innovation. Decentralized trust systems are difficult because participants to a transaction may be untrustworthy, and without the involvement of a trusted central institution like a bank, parties face increased risk that the other will not comply with the agreement. Especially when there is a financial incentive to cheat or lie, some actors can be expected to do so. If there

---

blockchain. And therefore, unlike traditional financial transactions where the parties may not know identities but some intermediaries, like banks, do, the actual identity of those transacting may be effectively impossible to determine.

73. J. DAX HANSEN, JACOB FARBER & PATRICK MURCK, PERKINS COIE LLP, BITCOIN: A PRIMER 2–4, <https://www.perkinscoie.com/images/content/1/4/v2/14394/Bitcoin-Primer.pdf> [<https://perma.cc/6AWT-Z6T2>]. Some distributed ledger systems use data structures other than blockchains, but the basic approach is similar.

74. Making the ledger public enhances trust because no one can hide or lie about the status of any transaction. Permissioned blockchains, which are limited to identified users, do not necessarily offer the global visibility of Bitcoin. See *infra* notes 269–71 and accompanying text.

75. The technical meaning of immutability for a blockchain is actually somewhat complex. See Angela Walch, *The Path of the Blockchain Lexicon (and the Law)*, 36 REV. BANKING & FIN. L. 713, 734–45 (2017).

76. See NARAYANAN ET AL., *supra* note 12, at 8.

77. See *id.*, at 53; Nakamoto, *supra* note 3, at 3–4.

78. Individuals wanting complete independence from any intermediary can, however, still operate their own full node on the network.

79. See NARAYANAN ET AL., *supra* note 12, at 52–61.

is a realistic possibility that malicious actors on the Bitcoin network could steal currency, or spend the same Bitcoins multiple times,<sup>80</sup> legitimate users and firms would be reluctant to use Bitcoin.

The great innovation in Bitcoin is to flip the incentive structure, by giving network nodes a reason to follow the legitimate consensus rather than behave dishonestly.<sup>81</sup> Bitcoin's approach to consensus is known as mining.<sup>82</sup> Bitcoin nodes repeatedly attempt to solve cryptographic hashing puzzles based on the transactions in a proposed new block on the blockchain. These puzzles are on a sliding level of difficulty so that, roughly every ten minutes, a random node finds a solution.<sup>83</sup> The new block based on that solution is broadcast across the network.<sup>84</sup> Other nodes, after checking for validity, add the new block to the blockchain.<sup>85</sup> In the event of conflicts, they follow the longest chain, which is the one the majority of the network supports. The node that successfully proposes the new block receives a financial reward.

These rewards for mining make Bitcoin resistant to attacks. Miners have incentives to apply as much computing power as possible to confirm valid blocks, because that increases their chance of winning the block reward.<sup>86</sup> Malicious actors are effectively competing against the total computing power in the network. Their blocks will only be adopted if they can solve the hashing puzzle before someone else. And

---

80. This is known as a double-spend transaction, and is effectively printing money.

81. See NARAYANAN ET AL., *supra* note 12, at 61–68; Nakamoto, *supra* note 3, at 4.

82. The more technical term for the mining process is Proof of Work. See Nakamoto, *supra* note 3, at 3.

83. See Adam Back, *A Partial Hash Collision Based Postage Scheme*, HASHCASH (Mar. 28, 1997), <http://www.hashcash.org/papers/announce.txt> [<https://perma.cc/DBV8-PR87>] (describing a proof of work system to combat email spam). Because nodes must essentially use brute force to solve the puzzles, their probability of success is proportional to their computing power. However, which node finds a valid solution first is essentially random.

84. See NARAYANAN ET AL., *supra* note 12, at 53.

85. The network includes additional mechanisms to deal with situations where more than one valid block is proposed, whether due to an attack or network latency. Every block in the blockchain is cryptographically linked to the block before. Under the Bitcoin protocol, when given the choice, nodes add a block to the longest possible blockchain. Every new block added thus increases the confidence level that prior blocks represent the consensus. The common heuristic in Bitcoin is that after six subsequent blocks (approximately one hour), nodes can be sufficiently confident that a block will not be replaced. In Bitcoin, however, trust is probabilistic, not absolute. Applications requiring greater security might wait longer before accepting transactions from a block, but the trade-off is increased delay before they transfer the Bitcoins or associated assets.

86. Cf. Kevin Werbach, *Bitcoin Is Gamification*, MEDIUM (Aug. 5, 2014), <https://medium.com/@kwerb/bitcoin-is-gamification-e85c6a6eea22> [<https://perma.cc/Q4Q8-4YGG>] (explaining the significance of the motivational system to Bitcoin).

because every block is linked to the previous one, as the chain gets longer, it becomes more and more difficult to replace an earlier set of transactions.

An elegant aspect of Bitcoin's mining system is that those financial rewards take the form of Bitcoins themselves.<sup>87</sup> Because Bitcoin is accepted as a currency, and can also be exchanged for traditional currencies, miners find the rewards desirable. Yet, the only reason Bitcoin has those properties is the trust generated by mining. Mining is, in fact, the only way that new Bitcoins are created. The mining reward is halved approximately every four years, meaning there will ultimately be no more than approximately 21 million Bitcoins ever created.<sup>88</sup> As an alternative compensation mechanism, Bitcoin allows parties to specify transaction rewards, which are deducted from the value of a validated transaction.<sup>89</sup> The expectation is that, as the available mining rewards decrease, voluntary transaction rewards will become the predominant incentive for Bitcoin miners.<sup>90</sup>

The combination of the ledger, the network, and consensus replaces authorities like financial or central banks, which traditionally serve to reinforce trust between transacting parties. If, for example, Abby commits to paying Bob one Bitcoin every year as a dividend for each share of stock Bob holds in Abby's company, every distributed ledger in the network will correctly reflect that information, because it will be encoded into a block of transactions that is immutably linked into a sequence. At no point in the future can anyone manipulate the

---

87. See NARAYANAN ET AL., *supra* note 12, at 62; Nakamoto, *supra* note 3, at 4. The block reward as of mid-2017 is 12.5 Bitcoins, which equates to roughly \$25,000 at contemporary exchange rates.

88. See *id.*, at 63. This enforced scarcity is necessary to support Bitcoin's value as a currency. If the number of Bitcoins could keep growing indefinitely, the currency would be subject to massive devaluation due to inflation. The Bitcoin protocol allows Bitcoins to be subdivided down to eight decimal places, with the smallest unit being designated as one Satoshi. So, even though the exchange rate of a Bitcoin is, as of mid-2017, over \$2,000, transactions can involve tiny amounts of money, far smaller than the equivalent of one cent.

89. Nakamoto called these "transaction fees." See Nakamoto, *supra* note 3, at 4. We use "transaction rewards" to clarify that the sum is offered by the transacting party, and only paid to the node that successfully validates a block through the mining process. It is not a fee specified by nodes in order to process a block.

90. See *id.* In practice, transaction rewards have grown rapidly because the Bitcoin system has struggled to keep up with growth. Users need to attach significant rewards to incentivize miners to process their transactions quickly. See Joseph Young, *As Recommended Fees Go Past \$2, Bitcoin Direly Needs a Scaling Solution*, CRYPTOCOINS NEWS (May 31, 2017), <https://www.cryptocoinsnews.com/urgent-necessity-of-a-scaling-solution-recommended-bitcoin-fees-go-past-2/> [<https://perma.cc/BSR9-BXX6>].

ledger to change or delete the transaction. Abby and Bob both know this and do not need a bank to provide reassurance that the Bitcoin transaction is legitimate. As the recipient of the dividend payment, Bob can confidently spend that Bitcoin without concerns about its legitimacy.

### C. Blockchain-Based Smart Contracts

As thus described, the blockchain is a general-purpose technology for trusted transactions. One important class of trusted transactions is contracts. A legally enforceable contract enables parties to coordinate their actions and trust that their commitments to each other will be fulfilled.<sup>91</sup> An inherent constraint on traditional contracting is that the parties must trust the state, and a variety of private intermediaries that facilitate efficient operation of the system. Legal enforcement of contracts can be cumbersome and prone to error. Just as there are reasons to use a decentralized digital currency system even though traditional currencies are successful, there are reasons to use decentralized digital contracts to solve problems that the conventional contract system cannot. The basic challenge for decentralized contracts is the same as for currencies: reliably ensuring that participants will follow the rules and accept their outputs.<sup>92</sup>

Szabo's original conception of smart contracts envisioned that cryptography would secure agreements, but had no mechanism to guarantee enforcement or transfer of value. Everything changed with the development of Bitcoin.<sup>93</sup> Bitcoin's success in decentralizing trusted financial transactions gives hope to those who advocate similar

---

91. See, e.g., Anthony J. Bellia Jr., *Promises, Trust, and Contract Law*, 47 AM. J. JURIS. 25, 26 (2002) ("The incentive to rely on a promise exists only to the degree that a promise is trustworthy."). As Stewart Macaulay famously showed, enforceable contracts enable coordination by structuring the relationship between contracting parties, even where threats of legal action are rare. See Stewart Macaulay, *Non-Contractual Relations in Business: A Preliminary Study*, 28 AM. SOC. REV. 55, 57 (1963); cf. Carolina Camén, Patrik Gottfridsson & Bo Rundh, *To Trust or Not To Trust?: Formal Contracts and the Building of Long-Term Relationships*, 49 MGMT. DECISION 365, 365 (2011) (studying empirically the role that formal contracts can play in cultivating trust). The theory behind smart contracts is built on this idea. See Szabo, *supra* note 2.

92. See FRANÇOIS R. VELDE, THE FED. RESERVE BANK OF CHI., BITCOIN: A PRIMER 1, 2–3 (2013) (stating that currencies "derive their value in exchange either from government fiat or from the belief that they may be accepted by someone else").

93. Jay Cassano, *What Are Smart Contracts? Cryptocurrency's Killer App*, FAST COMPANY (Sept. 17, 2014), <http://www.fastcolabs.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app> [<https://perma.cc/P7LX-9UFZ>]; David Z. Morris, *Bitcoin Is Not Just Digital Currency. It's Napster for Finance*, FORTUNE (Jan. 21, 2014), <http://fortune.com/2014/01/21/bitcoin-is-not-just-digital-currency-its-napster-for-finance> [<https://perma.cc/UV8E-U3X6>].

decentralization of trusted contractual agreements.<sup>94</sup> Smart contracts may actually be a bigger idea than Bitcoin as a currency.<sup>95</sup> They take the static ledger and turn it into a dynamic system capable of executing the business logic of a contractual agreement.

Consider a simple insurance contract under which Abby promises farmer Bob, in return for a monthly payment, a lump sum in the event the temperature exceeds 100 degrees for more than five straight days during the term of the agreement. In a traditional contracting arrangement, the parties would likely reduce that agreement to a writing, signed to memorialize mutual intent. If the temperature exceeded the threshold for six straight days and Abby failed to pay, Bob could file suit for breach and present the contract as evidence. To implement a smart contract with the same terms, Abby and Bob would translate the provisions into software code. Each would make available sufficient funds to fulfill his or her side of the agreement. An agreed mechanism would be specified to determine performance, such as the daily high temperature for the area, as published on Weather.com. Abby and Bob would then each digitally sign the agreement with their private cryptographic key. One of them would send it as a transaction onto a blockchain, where it would be validated through the consensus process and recorded on the distributed ledger. Bob's payments would automatically be deducted each month and credited to Abby's account. Meanwhile, the smart contract would check the high temperature on Weather.com each day and store a record as needed on the blockchain. If the temperature exceeded 100 degrees for six days, the lump sum payment would be transferred from Abby's account to Bob's, and the smart contract would terminate.

The critical distinction between smart contracts and other forms of electronic agreements is enforcement. Once the computers determine that the requisite state has been achieved, they automatically perform data-oriented or computable contracts.

---

94. Nick Szabo, *Foreword* to CHAMBER OF DIG. COMMERCE, SMART CONTRACTS: 12 USE CASES FOR BUSINESS & BEYOND 3 (2016), <http://www.the-blockchain.com/docs/Smart%20Contracts%20%2012%20Use%20Cases%20for%20Business%20and%20Beyond%20%20Chamber%20of%20Digital%20Commerce.pdf> [https://perma.cc/9ZZT-9NX8] (“Blockchain technology appears very much to be the jet fuel necessary for smart contracts to become commonplace in business transactions and beyond.”).

95. See Cassano, *supra* note 93. The currency aspect of Bitcoin is necessary, regardless of the application, because it provides the incentive structure for mining, at least in the ramp-up stage before transaction fees become dominant. Conceivably, Bitcoin could fail to have a significant impact on the financial system but still be the basis for the massive adoption of smart contracts.

Humans can interrupt that execution at any point.<sup>96</sup> But with a smart contract, complete execution of the agreement, including any transfer of value, occurs without any such opportunity to interrupt.<sup>97</sup> Accordingly, juridical forums are powerless to stop the execution of smart contracts—there is no room to bring an action for breach when breach is impossible. The computers in the blockchain network ensure performance, rather than any appendage of the state.<sup>98</sup> And, because blockchains run on a distributed network of independent nodes, with no central control point,<sup>99</sup> a litigant seeking to enjoin performance of a smart contract has no one to sue.<sup>100</sup>

---

96. If a contract is executed on a traditional centralized computer system, the organization in control of that system can always stop execution. On a blockchain, no single entity controls the execution process. Furthermore, the output of a data-oriented or computable contract is at best only of provisional legal value. *See* Surden, *supra* note 15, at 637 n.25 (“[A]utomated assessments will often be ‘first cut’ approximations of an ultimate, legally authoritative determination as to compliance.”).

97. *See infra* Part II.B.3. The only exception to immutable execution of a smart contract is a fork which splits the entire blockchain into incompatible tracks. If enough network nodes follow the track without the smart contract, it effectively no longer exists. However, such a move is so technically and politically costly that it rarely if ever occurs on functioning blockchains. *See infra* note 177 and accompanying text.

98. *See* Karen E.C. Levy, *Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and the Social Workings of Law*, 3 ENGAGING SCI., TECH. & SOC’Y. 1, 2 (2017) (“Because they are based on code, smart contracts can be *immediately and automatically* effectuated, without . . . the intervention of institutions like courts.”). The power of the smart contract is, however, limited to those assets which can be incorporated or controlled by a blockchain. A smart contract for construction of a house could not force the builder to perform, for example, nor could a smart contract to purchase a painting physically move it to the buyer’s home. With techniques such as “smart property,” however, more assets will be susceptible to blockchain control. *See* Fairfield, *supra* note 57, at 825–28.

99. The organizations developing the blockchain’s software have no power over the network nodes that validate transactions. Even if a court ordered the software developers to issue an update that halted a particular smart contract, the miners would not have to adopt it. And because anyone around the world can set up a mining node on a public blockchain such as Bitcoin or Ethereum, there would be no way for that court to enforce compliance by the miners.

Exactly how powerless a court would be depends on the system. It is possible to use the basic technical approach of a blockchain to execute smart contracts on a “permissioned” network in which nodes must be authenticated and approved. *See* Tim Swanson, *Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems*, GREAT WALL OF NUMBERS (Apr. 6, 2015), <http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf> [<https://perma.cc/V36W-EFPA>]. Those nodes could be contractually bound to follow duly issued judicial decisions. Even in that scenario, the practicalities of judicial oversight of the contract could be quite challenging. Further, it is unclear why a permissioned blockchain network would deliberately compromise the automation and certainty upon which the efficiency gains of smart contracts are premised.

100. Operators of sites connected to a blockchain, such as the infamous Silk Road online marketplace for illegal transactions using Bitcoin, may be brought to the bar. Silk Road operator Ross Ulbricht was eventually caught by U.S. law enforcement authorities and sentenced to life in

The blockchain's distributed trust facilitates smart contracts between unknown or untrusted counterparties.<sup>101</sup> This radical decentralization is what potentially makes smart contracting a substitute for the state-based legal system, rather than an additional step before reaching that system. For example, a financial trading program that automatically buys certain stocks when prices match a predefined algorithm, could be described as a smart contract. If a dispute arises, however, the parties to that self-executing transaction will still turn to the courts, which will apply traditional legal doctrines to evaluate the agreement, ascertain breach, and impose a remedy if appropriate. With smart contracts, the transaction is irreversibly encoded on a distributed blockchain. A judicial decision holding a smart contract unenforceable cannot undo the results of its fully executed agreement.

Smart contracts are possible with Bitcoin because its protocols include a scripting language that can incorporate limited programmable logic into transactions.<sup>102</sup> The vast majority of transactions on the Bitcoin blockchain are simple transfers of Bitcoins between accounts.<sup>103</sup> Additionally, when computers on the Bitcoin network process those transfers, they can perform other functions.<sup>104</sup> This allows for more complicated arrangements, like delaying payment until a specified number of parties provide confirmation.

Bitcoin's native scripting language is limited. Companies are developing more powerful systems that execute the contractual logic on application servers outside the blockchain, or through alternate blockchains supporting more sophisticated scripts. The most heralded is Ethereum, a general-purpose computing platform on a blockchain foundation.<sup>105</sup> Ethereum is a competing system to Bitcoin. It uses the

---

prison. Kevin McCoy, *Silk Road Mastermind Ross Ulbricht Loses Legal Appeal*, USA TODAY (May 31, 2017, 11:30 AM), <https://www.usatoday.com/story/money/2017/05/31/silk-road-mastermind-ross-ulbricht-loses-legal-appeal/102343062> [<https://perma.cc/V56Q-SKGS>]. The blockchains themselves are another story.

101. See generally Werbach, *supra* note 17 (describing the blockchain's "trustless trust" architecture).

102. See NARAYANAN ET AL., *supra* note 12, at 79–84.

103. See *id.* at 82–83 (observing that 99.9 percent of Bitcoin transactions at the time were straight transfers of coins).

104. See *id.* at 84.

105. See Tina Amirtha, *Meet Ether, the Bitcoin-Like Cryptocurrency That Could Power the Internet of Things*, FAST COMPANY (May 21, 2015), <http://www.fastcompany.com/3046385/meet-ether-the-bitcoin-like-cryptocurrency-that-could-power-the-internet-of-things> [<https://perma.cc/77R6-ZE3F>]; *A Next-Generation Smart Contract and Decentralized Application Platform*,

same basic approach of a distributed ledger, a network of validation nodes, and consensus through mining. However, the virtual currency in the system, called Ether, is designed for purchasing computing power on the Ethereum network, rather than as an alternative to traditional currencies. Ethereum's scripting language is significantly more powerful than Bitcoin's. It is Turing complete, which means it can in theory execute any function that can be processed by a computer.<sup>106</sup>

The promise of Ethereum is almost comically broad: one article suggested it might "transform law, finance, and civil society."<sup>107</sup> While such enthusiasm may be excessive, Ethereum has gained a substantial and passionate following among developers and cryptocurrency enthusiasts. Roughly a year after Ethereum launched, there were already over three hundred distributed apps built on the platform.<sup>108</sup> In one of the largest crowdfunding campaigns to that point, Ethereum raised over \$18 million worth of Bitcoin in the initial sale of Ether.<sup>109</sup> A number of more specialized blockchain-based platforms employing smart contracts launched after Ethereum.

The scripting language on a blockchain platform like Bitcoin or Ethereum can be used to determine whether the conditions for performance of a smart contract have been met, and then execute the contractual transaction without human interference.<sup>110</sup> In the simplest case, parties place Bitcoins or other digital currency into a suspended state on the blockchain, and once certain terms are met, those Bitcoins are transferred to the appropriate account.<sup>111</sup> The Bitcoins may

---

GITHUB, <https://github.com/ethereum/wiki/wiki/White-Paper> [<https://perma.cc/4DLU-SJD3>]; Jim Epstein, *Here Comes Ethereum, an Information Technology Dreamed Up by a Wunderkind 19-Year-Old That Could One Day Transform Law, Finance, and Civil Society*, REASON.COM (Mar. 19, 2015), <http://reason.com/blog/2015/03/19/here-comes-ethereum-an-information-techn> [<https://perma.cc/X6QU-SK83>]; D.J. Pangburn, *The Humans Who Dream of Companies That Won't Need Us*, FAST COMPANY (June 19, 2015), <http://www.fastcompany.com/3047462/the-humans-who-dream-of-companies-that-wont-need-them> [<https://perma.cc/MW9R-CURA>].

106. See *A Next-Generation Smart Contract and Decentralized Application Platform*, *supra* note 105.

107. Epstein, *supra* note 105.

108. See STATE OF THE DAPPS, <http://dapps.ethercasts.com> [<https://perma.cc/4T99-URGE>].

109. Nathan Schneider, *After the Bitcoin Gold Rush*, NEW REPUBLIC (Feb. 24, 2015), <http://www.newrepublic.com/article/121089/how-small-bitcoin-miners-lose-crypto-currency-boom-bust-cycle> [<https://perma.cc/Z7UQ-ZCUZ>]. Even though Ether is not intended as a replacement for cash, it can be exchanged for other currencies at a floating rate. Demand for Ether, based on the utility of the Ethereum smart contract platform, makes the tokens more valuable.

110. See NARAYANAN, *supra* note 12, at 286–88.

111. See Cassano, *supra* note 93. Not all smart contracts require funds to be placed in this escrow state. First, many contracts do not involve direct transfers of funds. Second,



represent payment directly, or they may be used as tokens, associated with digital rights in assets.

This algorithmic enforcement allows contracts to be executed as quickly and cheaply as other computer code. Cost savings occur at every stage, from negotiation to enforcement, especially in replacing judicial enforcement with automated mechanisms.<sup>112</sup> If smart contracts are substantially cheaper and more efficient, more situations can benefit from the use of contractual agreements; for example, dynamic transactions around physical objects (smart property)<sup>113</sup> or offerings for those unable to afford traditional legal services.<sup>114</sup> Another broad attraction of smart contracts is their fundamentally decentralized nature. Those who wish to avoid trust in centralized private or governmental actors, for political reasons or otherwise, can do so and still benefit from the advantages of contract.

Even though blockchain transactions are irrevocable, there are ways to build in more flexibility. There is no technical means, short of undermining the integrity of the entire system, to unwind a transfer.<sup>115</sup> It is, however, possible to incorporate logic into a smart contract that permits exceptions or conditions.<sup>116</sup> Enforcement could theoretically be structured to permit arbitration.<sup>117</sup> Such flexibility, however, must be coded into the smart contract at the outset, which takes away from the decentralization and efficiency that make smart contracts attractive

---

cryptocurrency can be used as a token to designate other assets or rights, such as title to real property. Smart contract system developers are now working through the issues involved to apply smart contracts to more complex instruments such as financial derivatives, where counterparties typically do not prefund all transactions so as to maximize liquidity. *See* Luke Clancy, *Barclays Taps Blockchain for Equity Swaps, Options, Swaptions*, RISK.NET (May 16, 2016), <http://www.risk.net/derivatives/2457777/barclays-taps-blockchain-equity-swaps-options-swaptions> [https://perma.cc/VX56-JGYK].

112. Of course, there is a trade-off for the certainty of algorithmic enforcement, as will be discussed in *infra* Part IV.

113. *See* Fairfield, *supra* note 57, at 825–28; Cassano, *supra* note 93.

114. *See* Cassano, *supra* note 93.

115. *See* Paul Vigna, *Ethereum Gets Its Hard Fork, and the ‘Truth’ Gets Tested*, WALL. ST. J.: MONEYBEAT BLOG (July 20, 2016 10:56 AM), <http://blogs.wsj.com/moneybeat/2016/07/20/ethereum-gets-its-hard-fork-and-the-truth-gets-tested/> [https://perma.cc/8PXE-RBRG] (describing such a “hard fork” needed to unwind a fraudulent transaction on the Ethereum network).

116. These are simply additional terms of the contract conveyed through the scripting language of the blockchain system.

117. Pamela Morgan, *At Bitcoin South: Innovating Legal Systems Through Blockchain Technology*, BRAVE NEW COIN (Dec. 17, 2014), <http://bravenewcoin.com/news/pamela-morgan-at-bitcoin-south-innovating-legal-systems-through-blockchain-technology> [https://perma.cc/8446-WHPN].

to begin with.

Sometimes a smart contract refers to facts in the world, for example, when a contract pays out if a stock exceeds a certain price on a certain date. The Bitcoin blockchain knows nothing about stock prices; it must collect that information through an external data feed. In the language of smart contracts, systems that interpret such external feeds and verify contractual performance are called “oracles.”<sup>118</sup> Unlike the blockchain itself, oracles are not fully decentralized. The contracting parties must, to some degree, trust the operator of the oracle and the authenticity of its data feed.<sup>119</sup>

Using these capabilities, a wide variety of industries could employ smart contracts. Beyond simple financial arrangements, smart contracts could facilitate complex instruments like wills<sup>120</sup> or crowdfunding systems, both of which disburse funds only if certain contingencies trigger a payout.<sup>121</sup> Another category is smart property, for which the rights associated with objects attach to the objects themselves.<sup>122</sup> Networked door locks on a shared car system such as Zipcar could automatically open, but only for the individual that paid the access fee. Or, a lessor could shut off a delinquent lessee’s access to a leased car, and give access to the bank, but only until full payment of

---

118. See *Smart Oracles: A Simple, Powerful Approach to Smart Contracts*, GITHUB (July 17, 2014), <https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts> [<https://perma.cc/YWJ3-CQPQ>].

119. There are, however, efforts to create distributed oracles using blockchain-based prediction markets such as Augur and Gnosis, which use financial incentives and the wisdom of crowds to evaluate statements. See Cade Metz, *Forget Bitcoin. The Blockchain Could Reveal What’s True Today and Tomorrow*, WIRED (Mar. 22, 2017, 9:15 AM), <https://www.wired.com/2017/03/forget-bitcoin-blockchain-reveal-whats-true-today-tomorrow> [<https://perma.cc/828D-3R58>].

120. See Morris, *supra* note 93. A will implemented through smart contracts would specify the distribution of assets in the estate according to a set of rules. The contract could be activated with presentation of a specified private key by the executor of the estate. A hypothetical set of rules might transfer the entire balance of the estate to the private key associated with the decedent’s spouse. In the event the spouse was also deceased (as verified by the executor’s presentation of another private key), the funds would be divided equally among the decedent’s two children. This scenario would work most simply for assets held in the form of cryptocurrencies. However, the blockchain could also record access rights to bank accounts, title to real estate, or other tokens associated with traditional assets.

121. See Stan Higgins, *Bitcoin-Powered Crowdfunding App Lighthouse Has Launched*, COINDESK (Jan. 20, 2015), <http://www.coindesk.com/bitcoin-powered-crowdfunding-app-lighthouse-launches-open-beta/> [<https://perma.cc/W7WQ-9VLN>]; Paul Vigna & Michael J. Casey, *The Car of the Future May Ownerless as well as Driverless*, MARKETWATCH (Mar. 3, 2015), <http://www.marketwatch.com/story/how-bitcoin-technology-could-power-driverless-cars-2015-03-03> [<https://perma.cc/37NV-W5EL>].

122. See Fairfield, *supra* note 57, at 863.

the principal. More broadly, over twenty-five billion devices comprising the Internet of Things, from light switches to crop moisture monitors, are expected to connect to the internet by 2020.<sup>123</sup> Smart contracts would allow these devices to operate autonomously, share resources, and exchange data without central management.<sup>124</sup>

Some blockchain advocates go further. They envision smart contracts as the foundation of a new kind of economic entity, the distributed autonomous organization (DAO).<sup>125</sup> If a corporation is simply a nexus of contracts,<sup>126</sup> why not encode those agreements into digital self-enforcing agreements? A DAO could have stock ownership, corporate governance rules, payroll arrangements, and virtually all of the economic trappings of a modern corporation, all running automatically in a completely distributed manner.

With the success of Ethereum and other blockchain-based platforms offering smart contracting capabilities, Szabo's twenty-year-old hypothetical has become an operational reality. Over one hundred major corporations including JPMorgan Chase, IBM, BP, Microsoft, Toyota, and Merck, have joined a consortium to promote enterprise adoption of Ethereum.<sup>127</sup> Many others are supporting competing initiatives.<sup>128</sup>

As is so often the case, though, this technology's adoption is preceding full consideration of its legal implications. Smart contracts are not just an interesting computer science innovation, because they

---

123. See Colin Barker, *Is Blockchain the Key to the Internet of Things? IBM and Samsung Think It Might Just Be*, ZDNET (Jan. 21, 2015), <http://www.zdnet.com/article/is-blockchain-the-key-to-the-internet-of-things-ibm-and-samsung-think-it-might-just-be/> [https://perma.cc/SR5T-ERN4].

124. See *id.*

125. Vitalik Buterin, *Bootstrapping A Decentralized Autonomous Corporation: Part I*, BITCOIN MAG. (Sept. 19, 2013), <https://bitcoinmagazine.com/7050/bootstrapping-a-decentralized-autonomous-corporation-part-i> [https://perma.cc/V8ZY-NK2J]; David Johnston et al., *The General Theory of Decentralized Applications, Dapps*, GITHUB, <https://github.com/DavidJohnstonCEO/DecentralizedApplications> [https://perma.cc/4C9S-J3ZH].

126. Michael C. Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. FIN. ECON. 305, 311 (1976).

127. See Matthew Leising, *Toyota, Merck Join Ethereum Group To Build Blockchain Network*, BLOOMBERG (May 22, 2017, 12:00 AM), <https://www.bloomberg.com/news/articles/2017-05-22/toyota-merck-join-ethereum-group-to-build-blockchain-network> [https://perma.cc/GJ67-ZHKW].

128. See, e.g., Arjun Kharpal, *Intel and Major Banks, Including HSBC and BOAML, Pour \$107 Million Into Blockchain Group*, CNBC (May 23, 2017, 8:30 AM), <http://www.cnbc.com/2017/05/23/r3-funding-blockchain-intel-bank-of-america-hsbc.html> [https://perma.cc/SV2Y-GX54] (detailing new funding for the financial industry blockchain platform R3).

tread on one of the most fundamental territories of the common law: the domain of contract.

## II. CONCEPTUALIZING SMART CONTRACTS

### A. *Are Smart Contracts Contracts?*

The first important question that smart contracts pose is: Are they actually contracts? Ultimately, we think the answer is “yes.” But this question turns out to be ambiguous, requiring the answer to another question first: What do we mean by a “contract”? Different ways of defining contracts, in terms of legal enforceability, intent of the parties, or an exchange of promises, all complicate the analysis of whether smart contracts are contracts at all. After considering such standard definitions, we will suggest that smart contracts should nonetheless be considered contracts because they are agent-generated mechanisms to shift rights and obligations.

According to the standard legal definition, a contract is a promise or an agreement that is legally enforceable.<sup>129</sup> This definition, though widely accepted, has the unfortunate linguistic consequence of implying that agreements that turn out to be unenforceable were not contracts to begin with. Terms like “unconscionable contract,” “fraudulent contract,” and “illegal contract,” all become something like oxymorons.<sup>130</sup> Even commonplace judicial iterations of this standard, like “[t]o be legally enforceable, a contract must be supported by consideration,”<sup>131</sup> become essentially redundant.

But we care about whether smart contracts are contracts in the ordinary sense, whether they are enforceable or not.<sup>132</sup> At a general conceptual level, are smart contracts actually contracts? So it seems

---

129. *E.g.*, RESTATEMENT (SECOND) OF CONTRACTS § 1 (AM. LAW INST. 1981) (“A contract is a promise or a set of promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognizes as a duty.”).

130. *But cf., e.g.*, *United States v. Nunez*, 673 F.3d 661, 664 (7th Cir. 2012) (“[C]onspiracy’ . . . is simply a pejorative term for a contract, both ‘conspiracy’ and ‘contract’ signifying an agreement, a meeting of minds.”).

131. *See, e.g.*, *Hartbarger v. Frank Paxton Co.*, 857 P.2d 776, 780 (N.M. 1993) (“[T]o be legally enforceable, a contract must be factually supported by an offer, an acceptance, consideration, and mutual assent.”).

132. Along these lines, Thomas Joo distinguished between “Rs,” which are simply relationships of reciprocal expectations and behavior, and “Ks,” which are legally enforceable. *See* Thomas W. Joo, *Contract, Property, and the Role of Metaphor in Corporations Law*, 35 U.C. DAVIS L. REV. 779, 790 (2002). One way to pose the question that we are now asking would be: Are smart contracts Rs, whether or not they are Ks?

that we need a different definition of “contract” for these purposes.

One way to understand the question would be: Do smart contracts constitute promises or agreements that are *intended* to be legally enforceable? Corresponding to this formation of the question, another definition of a contract is an agreement intended to be legally enforceable, whether it turns out to be or not.<sup>133</sup> This definition has the advantage of avoiding the issues raised above, because it leaves open the question of enforceability. The unenforceable contract is still, conceptually, a contract as long as the parties thought that it would be enforceable, wrong though they may have been.

Of course, the intent that matters here is objective, not subjective, intent as it is manifested by the actions of the parties. As Judge Hand famously explained, “[a] contract has, strictly speaking, nothing to do with the personal, or individual, intent of the parties. A contract is an obligation attached by the mere force of law to certain acts of the parties, usually words, which ordinarily accompany and represent a known intent.”<sup>134</sup> Still, according to this understanding, a contract exists if and only if the actions of the parties, judged objectively, manifest an intention that an agreement is to be legally enforceable.

When applied to smart contracts, this definition raises a serious issue. Smart contracts are designed to eliminate the need for legal enforcement. The central feature of a smart contract—what supposedly makes them smart—is that legal enforcement will not be necessary, or even possible. In a very real way, smart contracts are *not* intended to be legally enforceable. This is not to suggest that they are intended to be legally invalid; rather, the question of legal enforcement should never arise. In this sense, smart contracts are *not* intended to be enforced in a legal proceeding. This lack of intent may lead to the conclusion that, even conceptually, smart contracts are not truly contracts at all. They may look more like so-called “gentlemen’s agreements,” intended to be carried out, but never intended to reach a

---

133. See, e.g., EARL OF HALSBURY, 7 LAWS OF ENGLAND § 682 (1909) (“A contract is an agreement made between two or more persons which is intended to be enforceable at law . . . .”); see also *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1108 (9th Cir. 2009) (“[O]nce a court concludes a promise is legally enforceable according to contract law, it has implicitly concluded that the promisor has manifestly intended that the court enforce his promise.”).

134. *Hotchkiss v. Nat’l City Bank*, 200 F. 287, 293 (S.D.N.Y. 1911); see also *Lucy v. Zehmer*, 84 S.E.2d 516, 522 (Va. 1954) (“If his words and acts, judged by a reasonable standard, manifest an intention to agree, it is immaterial what may be the real but unexpressed state of his mind.”); RESTATEMENT (SECOND) OF CONTRACTS § 17 cmt. c (AM. LAW INST. 1981) (“[I]t is clear that a mental reservation of a party to a bargain does not impair the obligation he purports to undertake.”).

courtroom.

This appearance would be misleading, however, because it is quite different to intend that a solution will not be needed than to intend that it will be unavailable. I do not intend that my car will be needed as a vehicle for escaping the zombie apocalypse, but if the zombie apocalypse comes, I do not intend to abandon my car and traverse the wasteland on foot. By the same token, smart contracts are not intended to be enforced by a court, but that's not to say that, if they end up in court, the parties intend them to be unenforceable.

It is better to think of a contract as any agreement that is meant to have practical consequences on the rights and duties of the parties—that is, is not merely aspirational.<sup>135</sup> This avoids the above difficulty, because whether legal enforcement was anticipated is irrelevant.<sup>136</sup> Smart contracts would be contracts as long as they manifest an exchange of concrete obligations. They would be contracts as long as they are meant to alter concretely the normative relation between the parties.

Yet there is still some difficulty with this definition, because this understanding of a contract requires an exchange of promises or obligations. Do smart contracts involve promises or obligations? In a significant sense, “no.” The smart contract sets in motion machinery that the parties cannot subsequently prevent. The smart contract is not fulfilled by some further action of a contracting party, but rather by the completion of this mechanical process. As an analogy, if Bob balances a pail of water on top of a door, he does not promise to drop water on whoever next opens the door. Rather, he has merely set up the mechanical process by which that will inevitably happen. In a similar way, a smart contract to transfer one Bitcoin upon such-and-such event occurring is not really a promise at all. A smart contract would not say, “I will pay you one Bitcoin if such-and-such happens,” but rather something like, “you will be paid one Bitcoin if such-and-such happens.”

---

135. See, e.g., W. David Rankin, *Concerning an Expectancy Based Remedial Theory of Promissory Estoppel*, 69 U. TORONTO FAC. L. REV. 116, 142 (2011) (“[A] contract creates rights and duties because, as purposive beings, self-determining agents may transfer the power to direct their choices to other persons, and rights and duties are required to mark the resultant scope of the parties’ freedom after the transfer.”).

136. See Gregory Klass, *Intent to Contract*, 95 VA. L. REV. 1437, 1460 (2009) (arguing that departure from any intention to create legal enforceability makes sense because “[c]ontracts create legal rights and duties” and “[t]he conditions of contractual validity function . . . to inform people of their rights and duties ex ante”).

Some of the computer scientists working on smart contracts appear to be vaguely aware of this point. For example, Ethereum’s white paper states that its contracts “should not be seen as something that should be ‘fulfilled’ or ‘complied with’; rather, they are more like ‘autonomous agents’ that live inside of the Ethereum execution environment.”<sup>137</sup> As this suggests, the language of “contracts” is a poor fit, because this sort of smart contract is not an exchange of promises or commitments. Creation of a smart contract—while setting certain events in motion—does not commit any party to do anything, or make any prospective promise.

Nevertheless, we believe that smart contracts are, at the conceptual level, still contracts.<sup>138</sup> Though they might not constitute promises per se, smart contracts are voluntary mechanisms that purport to alter the rights and duties of the parties. After all, not all traditional contracts are executory, either. A deal may still count as a contract even though it leaves nothing open to be done or performed. A conveyance, for example, is a contract that alters rights presently, and does not involve any further, open promises. Smart contracts similarly constitute present agreements without further promises to perform. The simple Bitcoin smart contract just imagined is more like a present but contingent conveyance than it is like an executory promise to pay.

Thus, the smart contract somewhat breaks down the traditional line between executory and executed contracts. Like the conveyance, there is no promise left to be performed. Unlike the conveyance, though, the smart contract does not transfer property at the time. It is neither executory, insofar as there is no action left to be performed, nor is it executed, insofar as the result is yet to be accomplished. This causes conceptual difficulty. Smart contracts are both committing to something in the future, but not exactly making a promise. As we discuss below,<sup>139</sup> this hybrid between ex ante commitment and ex post

---

137. *A Next-Generation Smart Contract and Decentralized Application Platform*, *supra* note 105; *see also Explainer: Smart Contracts*, *supra* note 14 (“[S]mart contracts are neither particularly smart nor are they, strictly speaking, contracts.”); Leithaus, Comment to *Isn’t Ethereum Just a DSL for the Blockchain?*, REDDIT.COM, [https://www.reddit.com/r/ethereum/comments/31rnmh/isnt\\_ethereum\\_just\\_a\\_dsl\\_for\\_the\\_blockchain/](https://www.reddit.com/r/ethereum/comments/31rnmh/isnt_ethereum_just_a_dsl_for_the_blockchain/) [<https://perma.cc/44DG-ZV54>] (“I now regret calling the objects in Ethereum ‘contracts’, [sic] as you’re meant to think of them as arbitrary programs and not smart contracts specifically.”).

138. For a more doctrinal analysis by an international law firm that reaches a similar conclusion, see NORTON ROSE FULBRIGHT LLP, *supra* note 12.

139. *See infra* Part II.B.3.

enforcement is novel.

In the end, though, this complication raises more questions about the conventional definitions of contracts than it does about whether smart contracts are contracts. There can be little doubt that smart contracts purport to alter the rights of the parties. The smart contract can explain, normatively as well as descriptively, why the Bitcoin belongs to one party and not the other. It constitutes an agreement between the parties, and not an idle one. That, we believe, is the essence of a contract. But it is an interesting conceptual observation—illuminated by the smart contract—that even yet-to-be-executed contracts need not create promissory obligations.

There is one final difficulty to overcome. Are smart contracts really agreements? After all, they are simply a chunk of code. Superficially, they may look nothing like a set of declarations in the form “Party X agrees to do such-and-such.” In general, a legal contract requires mutual assent, a “meeting of the minds,”<sup>140</sup> meaning that both parties must have expressed assent to the contract.<sup>141</sup> That is, contracts require overt acts of assent.<sup>142</sup> Parties must engage in some expression that displays a shared understanding of the agreement, and a shared intent to bind themselves by its terms. Can smart contracts, simply a chunk of code in a blockchain, constitute such shared expression?

Nothing, so far as we can tell, prevents an expression of mutual assent from being formulated in code.<sup>143</sup> In general, mutual assent can take many forms, so long as it clearly implies agreement.<sup>144</sup> As Surden puts it, “[a]t a minimum, contract laws do not explicitly prohibit expressing contractual obligations in terms of data. More affirmatively, basic contracting principles actively accommodate data-oriented

---

140. See, e.g., *Krasley v. Superior Court*, 161 Cal. Rptr. 629, 633 (Cal. Ct. App. 1980) (“The essence of a contract is the meeting of minds on the essential features of the agreement.” (citations omitted)).

141. See 1 ARTHUR LINTON CORBIN, CORBIN ON CONTRACTS § 4.13 (Matthew Bender & Co. 2017) (1950) (“[A contract requires] mutual expressions of assent to the exchange. These expressions . . . are external symbols of the thoughts and intentions of one party, symbols that convey these thoughts and intentions to the mind of the other party.”).

142. See, e.g., *Kitzke v. Turnidge*, 307 P.2d 522, 527 (Or. 1957) (“The law of contracts is not concerned with the parties’ undisclosed intents and ideas. It gives heed only to their communications and overt acts.”).

143. We are assuming the parties have some understanding of what the code is intended to accomplish. As Scholz points out, they could essentially agree to agree, and let the algorithms do the rest. This may be the case with some computable contracts today, as in the case of high-frequency trading. See Scholz, *supra* note 33. However, this is not an inherent problem with smart contracts, whose key differentiation lies in complete enforcement.

144. See RESTATEMENT (SECOND) OF CONTRACTS § 4 & illus. 1 & 2 (AM. LAW INST. 1981).



representation.”<sup>145</sup> In the present context, such data-oriented representations could easily include a blockchain. Where one party puts on the blockchain that assets of theirs will transfer to another party if some condition is satisfied, that seems to easily satisfy the requirement of an expression of assent.

This description in terms of a party putting the code on the blockchain does point to a wrinkle. Smart contracts, on Ethereum and presumably on other platforms, are by default unilateral, because only one party places them on the blockchain.<sup>146</sup> That is, the default involves one party specifying a transfer to another if certain conditions are met. Out of this default, one could approximate a bilateral or multilateral contract through the creation of two or more interrelated unilateral contracts.<sup>147</sup> But two unilateral contracts are not precisely the same as a bilateral contract.<sup>148</sup> Fashioning interdependent conditions in a way that would emulate a bilateral contract might be a challenge for smart contracts. But for the purposes of this Article, we will leave this issue aside and generally focus on unilateral contracts, because we think the same basic analysis would apply to bilateral contracts as they might be formulated as smart contracts.

To sum up, smart contracts are contracts. They are agreements to shift legal rights and responsibilities, no less than an agreement between two parties physically exchanging goods for payment over a counter. Their status as contracts might be obscured by the fact that the parties intend litigation to be impossible, may not make any promise, and may be expressed only in code. We suggest that these details do not alter the fact that smart contracts are, indeed, contracts in the important sense.

### *B. What’s New Here?*

Is a smart contract really any different than an ordinary one? The fact that smart contracts manifest agreements in machine-readable code is not novel, and neither is the possibility of automated performance based on rules-based judgments by computers. Both are

---

145. Surden, *supra* note 15, at 656.

146. See Raskin, *supra* note 23, at 314; Casey Kuhlman, Legal Approaches to Smart Contract Development (Apr. 9, 2014), <https://www.youtube.com/watch?v=wnFqOfR5a7I#t=29m25s>.

147. *Id.*

148. See Francesco Parisi, Barbara Luppi & Vincy Fon, *Optimal Remedies for Bilateral Contracts*, 40 J. LEGAL STUD. 245, 247 (2011) (illustrating from an economic perspective that, “contrary to intuition, the incentives faced in a bilateral contract are different from those that the parties would face if entering into two separate unilateral contracts”).

features of data-oriented and computable contracts, which have been around for some time.<sup>149</sup> And just because smart contracts are being implemented today on the exotic technology of the blockchain does not mean they raise novel or interesting legal issues. As Judge Frank Easterbrook has argued, new technologies do not necessarily call for new legal doctrines, when fact patterns are fundamentally unchanged.<sup>150</sup>

We consider two perspectives suggesting that smart contracts are just technological manifestations of familiar contractual processes: escrow and self-help. One perspective focuses on the mechanism smart contracts use to ensure the execution of agreements, and the other perspective focuses on the way smart contracts employ technology to impose a remedy outside of the court system. Each perspective sheds light on the nature of smart contracts. However, neither perspective fully captures the way smart contracts operate. Smart contracts are distinct from preexisting forms because the digital code is not just a representation of the agreement; it is the agreement.

1. *Smart Contracts as Escrow.* One could view smart contracts as simple escrow arrangements with a digital veneer. In a typical escrow agreement, such as a house purchase, the buyer places funds in a special account. The escrow agent can only withdraw and disburse these funds to the seller after successful inspection and resolution of any other prepurchase issues. More generally, escrow suspends execution of a valid contract, and empowers a trusted third party to complete the process. Among other attributes, this approach overcomes the possibility of a prisoner's dilemma when the parties do not fully trust one another; otherwise, whichever one acted first would be vulnerable. The escrow arrangement substitutes mutual trust in the escrow agent for bilateral trust between the parties.

Smart contracts mimic the functionality of escrow. The smart contract code can place Bitcoins or other cryptocurrency tokens in a suspended state on the blockchain, where they cannot be spent until performance of the contract.<sup>151</sup> The execution step may be fully

---

149. See *supra* Part I.A.

150. See Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 208. Judge Easterbrook was surely correct about this general point, but he may not have won the particular debate about the viability of cyberlaw. See Kevin Werbach, *The Song Remains the Same: What Cyberlaw Might Teach the Next Internet Economy*, 69 FLA. L. REV. (forthcoming 2017).

151. See NARAYANAN ET AL., *supra* note 12, at 84–85 (explaining how Bitcoin scripts can

automated, or it may be implemented through multiple-signature verification, known as multisig.<sup>152</sup> In order for a multisig smart contract to execute, more than one party must provide its private encryption keys, indicating approval to execute the previously agreed-upon transaction.<sup>153</sup> If Abby wishes to purchase digital goods from Bob using a smart contract, the parties can use a multisig smart contract, for which the ultimate execution requires the digital signatures of two out of three parties, typically the buyer, the seller, and a trusted third party, such as an arbitrator. If the contract is satisfactory, the buyer and seller sign, executing the terms of the contract. If either party refuses, claiming breach, the arbitrator's signature decides the outcome.

Startups are already using the sophisticated capabilities of smart contracts to apply escrow in new ways. For example, CryptoCorp uses multisig for preclearance checks on Bitcoin transactions, similar to the way credit card companies decline transactions if the card has been subject to fraud or the payment exceeds preset limits.<sup>154</sup> BitHalo has implemented an escrow system for e-commerce transactions that avoids the participation of third parties entirely, by requiring collateral to be stored on the blockchain.<sup>155</sup>

The fact that smart contracts can implement escrow agreements does not make them identical to escrow. Conventional escrow depends upon a trusted firm or third party, because the parties themselves cannot serve as the escrow agents. A smart contract reliant on an arbitrator gives up the decentralized trust that the blockchain makes possible. Smart contracts performing only escrow-like functions are therefore more like standard data-oriented contracts. A true smart contract may employ the escrow-like mechanism of holding Bitcoins temporarily, but it does so through automated execution of scripts running on the network of computers maintaining the blockchain, without an escrow agent equivalent.

---

mimic escrow transactions); Cassano, *supra* note 93.

152. See Ben Davenport, *What Is Multi-Sig, and What Can It Do?*, COIN CENTER (Jan. 1, 2015), <https://coincenter.org/2015/01/multi-sig/> [<https://perma.cc/W4VN-HTQT>].

153. See NARAYANAN ET AL., *supra* note 12, at 80.

154. See John Villasenor, *Could "Multisig" Help Bring Consumer Protection to Bitcoin Transactions?*, FORBES (Mar. 28, 2014, 9:43 PM), <http://www.forbes.com/sites/johnvillasenor/2014/03/28/could-multisig-help-bring-consumer-protection-to-bitcoin-transactions/> [<https://perma.cc/QGG8-LAXB>].

155. See Diana Ngo, *BitHalo Releases Decentralized Escrow Client v2.1 to Rival PayPal, Western Union*, COINTELEGRAPH (Jan. 12, 2015), <http://cointelegraph.com/news/113286/bithalo-releases-decentralized-escrow-client-v21-to-rival-paypal-western-union> [<https://perma.cc/JY2K-CVCB>].

2. *Smart Contracts as Self-Help*. Researcher Max Raskin provides a different interpretation of smart contracts. He views them not as legal enforcement at all, but as a form of self-help.<sup>156</sup> To Raskin, “[a]utomated execution of a contract is a preemptive form of self-help because no recourse to a court is needed for the machine to execute the agreement.”<sup>157</sup> He draws an analogy to starter interrupters, which are remote-controlled devices installed in cars to prevent them from operating.<sup>158</sup> A creditor can invoke the starter interrupter if the lessee of the car fails to pay. As Raskin notes, such devices are likely to be legal in most states, under the self-help repossession provisions for secured creditors at Section 9-609 of the UCC.<sup>159</sup> A smart contract could serve the same function, by refusing to authorize operation of the car unless the creditor receives payment.

Viewing smart contracts as self-help mechanisms accurately places the emphasis on the ex post enforcement function.<sup>160</sup> The blockchain can be used to record contractual provisions, execute contractual obligations, and perform intermediary functions like escrow, but so can garden-variety digital contracts. It is only when disputes arise, or when the remedies provided in the contract must be invoked, that smart contracts do something special. The algorithmic enforcement mechanisms, running automatically on the blockchain computing fabric, replace judicial enforcement.<sup>161</sup>

Self-help, traditionally, is a judicially supervised process.<sup>162</sup> Courts may restrain creditors from “disturbing the peace” to enforce their self-help rights, for example, or if a creditor’s rights are inferior to other legal obligations, such as those of bankruptcy.<sup>163</sup> With a smart contract, there is no one to restrain, because the smart contract code is

---

156. See Raskin, *supra* note 23, at 306 (“Over the past few years, a group of innovators have begun designing computer technologies that bring self-help to the realm of contracts. They call these new contracts ‘smart contracts.’”).

157. *Id.* at 333.

158. See *id.* at 329–33.

159. See *id.* at 332.

160. See Zoë Sinel, *De-Ciphering Self-Help*, 67 U. TORONTO L.J. 31, 58–65 (2017) (explaining that self-help, properly understood, is responding to a committed wrong, and that ex ante measures are not properly considered self-help because they are not so responding).

161. See *supra* Part I.C.

162. See Sinel, *supra* note 160, at 66–67 (“[S]elf-help is a [limited] privilege . . . . Only the state’s legal institutions (which include legally recognized agreements between two parties – that is, contracts) can effect [it] . . . . As such, self-help is not an alternative to the civil justice system but rather one small part of it.”).

163. See Raskin, *supra* note 23, at 310.

immutable once embedded in the blockchain. A smart contract could even include terms that are illegal, unconscionable, or otherwise legally unenforceable.<sup>164</sup>

More deeply, the self-help model focuses on what smart contracts *do* to the exclusion of what they *say*. Functionally, the primary distinction between smart contracts and more limited data-oriented or computable contracts lies in enforcement. The smart contract, as we have explained, fully executes the agreement. It addresses the possibility of breach, not through the deterrent potential of judicial remedies, but by making breach practically impossible. The smart contract is not merely an accessory added to the end of the contractual process to mitigate the risk of breach.

Raskin's analogy between smart contracts and starter interrupters breaks down on closer examination. The starter interrupter is a mechanism introduced, after an agreement is reached, to enforce its terms; but, unlike smart contracts, this mechanism has nothing to do with the substance of the agreement. By contrast, a smart contract literally contains the terms of the agreement, transformed into machine-readable scripting code. The fact that the agreement is enforceable algorithmically, without the participation of legal institutions, is a commitment represented in the smart contract. Thus, the self-help model paints too limited a picture of smart contracts.

At the same time, the self-help model is too expansive. This analogy attributes functions to smart contracts that they do not actually perform; the smart contract itself does not perform the breach-limiting action, the blockchain and its computing nodes do. In the self-help model, by contrast, one party enforces the agreement consistent with, but *outside* the legal machinery of contract law. The smart contract is a component of a larger smart contract system, which ensures that, for example, the cryptocurrency tokens are transferred according to the contractual terms. Just as the state's *ex post* remediation role distinguishes a legal contract from an informal exchange of promises,<sup>165</sup>

---

164. Raskin's proposed solution to the possibility of illegal smart contracts is to suggest that some forms of smart contracts be prohibited through regulation. *See* Raskin, *supra* note 23, at 340. This begs practical questions about enforcement. Smart contract platforms on public blockchains, such as Ethereum and Bitcoin, are open-source software adopted voluntarily by networks of mining node operators. There is not a central smart contract administrator to regulate. And the fact that identity on the blockchain generally takes the form of digital signatures rather than real names means it may not be feasible even to identify the counterparty who created an undesirable smart contract.

165. *See infra* Part III.C.

the integration of specific contractual terms and a general enforcement infrastructure makes a smart contract smart. The distributed ledger software both instantiates the contractual terms and enforces the contractual obligations. These functions are distinguishable, but necessarily connected.

3. *Smart Contracts as Entire Agreements.* Both the escrow model and the self-help model explain smart contracts as technical mechanisms overlaid on the basic contractual process. Escrow does so to facilitate performance, while self-help provides a remedy for nonperformance. These tools may reduce transaction costs and thereby make contracting more efficient. They are not, however, strictly necessary to the outcome. Neither fully captures the essence of smart contracts, because both treat smart contracts as external enhancements to the contractual process. The distinctive aspect of smart contracts is not that they make enforcement easier, it is that they make enforcement unavoidable. In order to do so, they change the nature of the contract itself.

In Szabo's vending machine example, the physical security of the device is sufficient to make breach less attractive than compliance.<sup>166</sup> But alongside physical security, another element is at work in Szabo's example. The vending machine takes cash, which is a bearer instrument. Once the coins or bills are in belly of the machine, value has been transferred. No third parties need to be brought into the process to facilitate or secure the exchange. Szabo's example does not easily translate to other payment mechanisms, like checks or credit cards, which require a bank to validate the transaction. This step introduces transaction costs and delay, and it means the contracting process is no longer contained within the hardware and software of the vending machine. And, intermediary validation potentially changes the performance equation. The consumer can breach the agreement by instructing the bank to reverse the charge, even after receiving the product. At that point, the smart contract would no longer govern the relationship between the parties.

Cash works for a vending machine, but not for complex financial derivatives transactions, international supply chains, or major crowdfunding initiatives. Only a limited subset of transactions are sufficiently localized, low value, and low velocity for cash to be a viable

---

166. See *supra* note 48 and accompanying text.

option.<sup>167</sup> For this reason, Bitcoin and other cryptocurrencies are very important for the growth of smart contracts. Bitcoin tokens are digital bearer instruments, functionally equivalent to cash, yet flexible and scalable in the manner of credit cards. A blockchain-based smart contract, like a cash transaction, therefore involves the complete exchange of value.

If I buy an e-book for my Kindle on Amazon.com, a complete transfer of value does not occur immediately. When I click the “buy” button, the company’s computers transfer the e-book to my device, with associated digital rights to prevent additional copying, and they also process my credit card and debit my account. Yet, I am in a position to prevent a complete transfer of value, because I can still ask Amazon for a refund, or dispute the charge with the credit card company. This is possible because my contract with Amazon is executory—I have traded the e-book for the promise to pay my credit card issuer. Imagining the same exchange with a smart contract, by contrast, it is as though when I click the buy button, a drone picks up a stack of one-dollar bills from my house and flies them to Amazon. The contract fully executes with no human intervention. I can still dispute the transaction with Amazon, but now the contract is fully executed. Amazon has the cash; I am now asking them to return the money, rather than preventing them from receiving it.

Because the exchange of value is entirely contained in the smart contract environment, there is no need to look anywhere else. In other words, the contract *is* the scripting code that tells the network what to transfer and when. In the Amazon example, the site’s computer system transfers the e-book and processes my credit card. Those machine instructions, however, are separate from my contract with Amazon, agreeing to exchange my payment information for a particular e-book.<sup>168</sup> If Amazon’s programmers make an error and send me an entirely different e-book, there is no question that my contract with

---

167. Or, they are transactions the parties do not want traced because they are somehow illicit. Unsurprisingly, one of the major early uses of Bitcoin was for illegal transactions. See Joshua Bearman, *The Rise and Fall of Silk Road: Part II*, WIRED (May 2015), <http://www.wired.com/2015/05/silk-road-2> [<http://perma.cc/4BCZ-LTBG>] (recounting the story of a Bitcoin exchange commonly used for drug sales and other illegal activity); Joshua Bearman, *The Rise and Fall of Silk Road: Part I*, WIRED (Apr. 2015), <http://www.wired.com/2015/04/silk-road-1> [<http://perma.cc/6BKF-BKY7>] (same).

168. There may be questions about what constitutes that contract. Perhaps it is a combination of what I saw on the shopping cart screen and Amazon’s Terms of Service, or perhaps some judicial gap filling is required. Under no circumstances, however, is the contract exclusively the software code executed on Amazon’s servers.

Amazon controls, rather than the software code the computer system uses to effectuate the contract.

For the smart contract, in contrast, everything beyond the code is just commentary. The code is a necessary part of the agreement itself, whereas Amazon's software code is just a tool to execute the human-made contract. For example, imagine that at the same time I place my order for the e-book on Amazon's website, I type up a written agreement for a different book and send it to an Amazon customer service agent, who countersigns it. In the event of a dispute, there would be an evidentiary question as to which version of the agreement controlled. In the smart contract context, such an inquiry would be meaningless. The smart contract has the entire life of the contract immutably embedded into its code, which leaves no room for a separate written agreement to specify the parties' intent. If a court concludes that some writing better reflects the parties' meeting of the minds, it would be powerless to invalidate the smart contract; it would have to find some way to reverse the transfer of value *ex post*.

The notion that smart contracts can supersede legal enforcement has been tested in the real world.<sup>169</sup> A group of developers associated with Ethereum created a distributed crowdfunding system in mid-2016 called "The DAO."<sup>170</sup> It was designed to implement the concept of DAO, in which corporate governance and operations are conducted automatically through smart contracts.<sup>171</sup> Users pledged Ether (the Ethereum cryptocurrency) in return for tokens that gave them authority to vote on projects to fund. Organizations seeking funding would sign up through another interface, and collect Ether if they received sufficient votes. Despite the novelty of the arrangement, Ethereum users pledged over \$150 million in Ether in a matter of weeks after The DAO launched.<sup>172</sup>

Users signed up to participate in The DAO on a website that stated explicitly, in its terms of service, that the smart contract on the

---

169. We note that whether smart contracts can displace contractual enforcement is a different question than whether, as we consider in Part III, they can displace contract law.

170. Christoph Jentzsch, *Decentralized Autonomous Organization to Automate Governance* (unpublished manuscript), <https://download.slock.it/public/DAO/WhitePaper.pdf> [<http://perma.cc/SE35-Y8CC>].

171. See *supra* note 125 and accompanying text.

172. Nathaniel Popper, *A Venture Fund With Plenty of Virtual Capital, but No Capitalist*, N.Y. TIMES (May 21, 2016), [http://www.nytimes.com/2016/05/22/business/dealbook/crypto-ether-bitcoin-currency.html?\\_r=0](http://www.nytimes.com/2016/05/22/business/dealbook/crypto-ether-bitcoin-currency.html?_r=0) [<https://perma.cc/2GP2-H9N7>].



Ethereum blockchain was the controlling legal authority.<sup>173</sup> Any human-readable documents or explanations, including those on the website, were “merely offered for educational purposes and do not supercede [sic] or modify the express terms of The DAO’s code set forth on the blockchain.”<sup>174</sup>

Within weeks of launch, something went wrong. A hacker took advantage of a bug in The DAO’s code to siphon off over \$60 million worth of Ether.<sup>175</sup> Although clearly an attempt at theft, the hack was executed through a series of smart contracts that were formally valid within the rules of The DAO. Even though the stolen funds were temporarily quarantined in an account, and not immediately disbursed, from the perspective of the smart contracting system, the transactions were perfectly legitimate. Even if a court ordered the funds returned, there was no one to carry out that order. Thus, there was no legal or technical way to recover them without undermining the entire system. Ultimately, the leaders of Ethereum project had to convince a majority of mining nodes to implement a “hard fork,” which split the entire Ethereum blockchain into two incompatible paths.<sup>176</sup> Only through this dramatic step, which effectively killed off The DAO and undermined confidence in the Ethereum platform, could the stolen funds be returned.<sup>177</sup>

---

173. The DAO’s original terms of service page, which was located at <https://daohub.org/explainer.html>, has been removed from the Web. For a contemporaneous quotation of the relevant language on the site, see Joel Ditz, *DAOs, Hacks and the Law*, MEDIUM (June 17, 2016), <https://medium.com/@Swarm/daos-hacks-and-the-law-eb6a33808e3e> [<https://perma.cc/N9M5-F2GT>].

174. *Id.*

175. Michael del Castillo, *The DAO Attacked: Code Issue Leads to \$60 Million Ether Theft*, COINDESK (June 17, 2016, 2:00 PM), <http://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/> [<https://perma.cc/3P4G-59MZ>]; Nathaniel Popper, *A Hacking of More than \$50 Million Dashes Hopes in the World of Virtual Currency*, N.Y. TIMES (June 17, 2016), [http://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html?\\_r=2](http://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html?_r=2) [<https://perma.cc/5NBQ-CFFN>]. The varying valuations of the hack are due to the floating exchange rate between Ether and dollars.

176. Miners of one chain do not recognize the validity of blocks mined by the other clients, and vice versa, even though they may otherwise use exactly the same protocols. See Joseph Bonneau et al., *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, IEEE TECHNICAL COMMITTEE ON SECURITY & PRIVACY 104, 113 (May 18, 2015), <http://www.ieee-security.org/TC/SP2015/papers-archived/6949a104.pdf> [<https://perma.cc/SWM8-MQZC>].

177. See Frances Coppola, *A Painful Lesson for the Ethereum Community*, FORBES (July 21, 2016, 1:54 PM), <https://www.forbes.com/sites/francescoppola/2016/07/21/a-painful-lesson-for-the-ethereum-community/#56d3a488bb24l> [<https://perma.cc/FRP2-7TDR>]. The hard fork was considered a “nuclear option” because it was not just a reversal of transactions by the operator of The DAO; it broke the fundamental immutability of transactions on the Ethereum blockchain.

The DAO example shows the power of smart contracts, and also their limitations. Smart contracts seemed to be able to replace the legal system as an enforcement mechanism for The DAO users' contractual relationship with the crowdfunding system. However, doing so came at a significant cost. Because the only enforcement mechanism was the Ethereum network's computers executing the terms of The DAO software code, there was no way to distinguish between a legitimate string of transactions and one with malicious intent.

### III. WHAT THEY TEACH US ABOUT CONTRACT LAW

As we have discussed, there are reasons to be skeptical about whether smart contracts can deliver all the hoped-for gains in efficiency and flexibility. But there is a much deeper, more theoretical reason to be skeptical of smart contracts. Even if the technology could deliver all that its proponents promise, it is not clear whether its implementation would be an improvement over courts or simply orthogonal. Put simply, the question is whether smart contracts could do what courts do, only better. We think not. Although we can see why some conclude otherwise, we think that contract litigation plays a role in our social system that smart contracts do not even purport to replicate.

Ostensibly, smart contracts remove the role of courts as enforcement agents. One might say that the contract enforces itself, or that the code itself enforces it. This means that parties no longer have the escape hatch of litigation. Once the smart contract is made, the machinery for its execution is unavoidably set in motion, ending the parties' opportunity to affect the transaction *ex post*.<sup>178</sup> This may be a bit of an overstatement. Parties can use multisig, for example, to

---

*See* Joon Ian Wong & Ian Kar, *Everything You Need to Know About the Ethereum "Hard Fork,"* QUARTZ (July 18, 2016), <https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/> [<https://perma.cc/B6DA-XC2L>] ("If contracts held to be inviolable can effectively be overturned by a collective decision to run new software, what guarantee do financial institutions have that their transactions and funds are secure?"). A faction of the Ethereum community considered this such a breach of trust that it began mining the deprecated chain on which The DAO hack was not reversed, creating a duplicate token called Ethereum Classic. *See* David Z. Morris, *The Bizarre Fallout of Ethereum's Epic Fail,* FORTUNE (Sept. 4, 2016), <http://fortune.com/2016/09/04/ethereum-fall-out> [<https://perma.cc/ZK78-NCJX>]. Broader questions about the legal or governance relationships among users, smart contract applications such as The DAO, and blockchain platforms such as Ethereum are beyond the scope of this Article. *See generally* Werbach, *supra* note 17 (discussing the governance implications of The DAO fiasco in connection with the trust architecture of the blockchain).

178. Note that this is consistent with the regular aim of business agreements to try to dictate remedies *ex ante*; for example, clauses pertaining to mandatory arbitration, choice of law/forum, disclaimer of incidental/consequential damages, among others.

maintain some control over the execution of the contract.<sup>179</sup> And in extreme cases such as The DAO hack, the entire blockchain could conceivably be forked if enough network nodes agreed.<sup>180</sup> Still, if smart contracts are to be a disruptive force in contracting, this potential turns on the ability to eliminate the possibility of breach and the resultant litigation to enforce.

Does this mean that smart contracts can replace courts in the adjudication of contract cases?<sup>181</sup> Courts, it might be argued, serve the function of enforcing contractual obligations. But, because courts serve this function in a costly and time-consuming way, technological advancement offers the possibility of making courts obsolete; surpassed by mechanisms that can enforce obligations, and serve the same function, with greater efficiency and customization.

Smart contracts thus offer a window into thinking about contract law at a theoretical level. Even if one were uninterested in the technology, smart contracts could illuminate foundational issues in the theory of contract. Their theoretical possibility, whether the technology can deliver or not, raises a pointed question about what function courts play when they adjudicate a contract case. Put another way, the basic question about whether smart contracts do what courts do, only better, introduces a reciprocal question about contract law more generally: Does contract law do what smart contracts aim to do? Taking smart contracts seriously is therefore a fruitful way to examine the function of courts and contract law.

In order to answer the question whether smart contracts can do what courts do, this Section describes three competing conceptions of what role courts play—or ought to play—in contract cases. Each view informs how its proponents think that smart contracts might interact with contract law. Ultimately, we argue that through the correct understanding of contract law, it is clear that smart contracts cannot supplant the role that courts play. Smart contracts are not, even conceptually, a replacement for judicial contract adjudication.

Our argument in this Section is bidirectional. Insofar as many readers may already intuitively grasp that smart contracts can, at best, avoid courts but cannot substitute for them, this Section provides the argument and reasoning to support that understanding.

---

179. NARAYANAN ET AL., *supra* note 12, at 62–63.

180. *See supra* note 175.

181. *See supra* notes 6–8 and accompanying text.

### A. *Contract Law as Enforcing Promises*

According to one view, contract law provides legal enforcement for promises.<sup>182</sup> When a promisor makes a commitment to a promisee, this commitment, the promise, generates an obligation to do the thing promised.<sup>183</sup> Even without contract law, a moral obligation is created when one party makes a promise to another. While the exact source of this moral obligation is subject of philosophical dispute, there is little doubt that promises generate obligations.<sup>184</sup> Contract law, the argument goes, serves to strengthen and support these moral obligations by creating corresponding legal obligations. At its core, contract law binds promisors, not simply morally, but also legally.

The paradigmatic articulation of the view that contract law enforces promises is Charles Fried's 1981 book, *Contract as Promise*.<sup>185</sup> For Fried, the capacity to make promises is a form of freedom, allowing parties to bind themselves and thus shape their obligations.<sup>186</sup> By enforcing such voluntarily assumed obligations, the state supports the freedom of contracting parties.<sup>187</sup> The core idea is that contracts are binding, as the self-imposed obligations of contracting parties. Contracts, like promises, are the result of voluntary acts performed with the intent to place the actor under an obligation. The ability to bind oneself in this way—to assume an obligation voluntarily—is itself a form of freedom. But one need not share Fried's account of

---

182. See generally CHARLES FRIED, *CONTRACT AS PROMISE: A THEORY OF CONTRACTUAL OBLIGATION* (1981) (grounding contract law in the morality of promises).

183. See, e.g., *id.* at 8 (“By promising we transform a choice that was morally neutral into one that is morally compelled.”).

184. Theoretical debate exists between convention-based views and reliance-based views. Conventionalist accounts understand promises as social conventions and understand their obligations as arising from the fact that failing to keep one's promise would do violence to a valuable social institution. See, e.g., DAVID HUME, *A TREATISE ON HUMAN NATURE* 524–25 (L.A. Selby-Bigge ed., 1967). Fried's account of contract law appeals to such a convention-based account of promises. FRIED, *supra* note 182, at 11–17. Convention-based accounts face a problem explaining the sense that promissory obligations are owed directly to the promisee, which can be explained better by appealing to the interests of the promisee. See T.M. SCANLON, *WHAT WE OWE TO EACH OTHER* 295–327 (1998). For a picture of contract law built on such a reliance-based account of promissory obligation, see generally Joseph Raz, *Promises in Morality and Law*, 95 HARV. L. REV. 916 (1982) (reviewing P.S. ATIYAH, *PROMISES, MORALS, AND LAW* (1981)). For further discussion of this philosophical debate, see generally WILLIAM VITEK, *PROMISING* (1993) and Niko Kolodny & R.J. Wallace, *Promises and Practices Revisited*, 31 PHIL. & PUB. AFF. 119 (2003).

185. FRIED, *supra* note 182, at 17–21.

186. *Id.* at 8.

187. *Id.* at 21.

promissory obligations in order to think that contract law's purpose is to provide legal obligations that correspond to the moral obligations of promises.<sup>188</sup>

The essential idea is that promises are an important part of human life, and that contract law supports promising by offering legal recognition and enforcement. Contract law layers legal obligation on top of our moral obligations in order to bolster them. By making it the case that a party must, legally, do what it has promised, we affirm that people ought to do what they promise, and we thereby affirm the institution of promising. The point of contract law, then, is to help ensure that people are truly bound by their promissory commitments.

From this perspective, contract law might appear incrementally more successful the more it affirms that promisors must do as they have promised. In this light, elements of contract law that diverge from ensuring that parties keep their promises may seem troubling.<sup>189</sup> Particularly, it may appear problematic that contract law generally imposes only expectation damages, rather than specific performance.<sup>190</sup> Specific performance more closely matches our moral obligation to do the thing promised.<sup>191</sup> Insofar as the point of contract law is to strengthen and affirm our moral obligations, and insofar as our moral obligations are to do as we have promised, then contract law should aim to align morality and legal obligation.

If one holds this conception of contract law's function, then smart contracts may seem like an appealing alternative to court-based contract law. Courts exert legal force upon us to do as we have promised, thus strengthening our voluntarily assumed commitments. But legal force is a relatively clumsy mechanism. If we want people to

---

188. See generally, e.g., T.M. Scanlon, *Promises and Contracts*, in *THE THEORY OF CONTRACT LAW* 86 (Peter Benson ed., 2001) (defending a view of contract law based on the importance of providing assurance to another that promising allows); Daniel Markovits, *Contract and Collaboration*, 113 *YALE L.J.* 1417 (2004) (defending a view of contract law based on the community created between promisor and promisee).

189. See, e.g., Seana Valentine Shiffrin, *The Divergence of Contract and Promise*, 120 *HARV. L. REV.* 708, 749 (2007) (noting the aim of "advanc[ing] an accommodationist approach that renders the norms of interpersonal morality relevant to the shape of law" and "deploy[ing] this approach to sound some alarms about the divergence of promise and contract, particularly with respect to contract's remedial doctrines").

190. *Id.* at 724 ("The law . . . fails to use its distinctive powers and modes of expression to mark the judgment that breach is impermissible as opposed to merely subject to a price.").

191. *Id.* at 722 ("Contract law would run parallel to morality if contract law rendered the same assessments of permissibility and impermissibility as the moral perspective, except that it would replace moral permissibility with legal permissibility and it would use its distinctive tools and techniques to express those judgments.").

do as they have promised, then a mechanism that automatically and completely ensures performance may look like a triumph, at least to the extent that it does not come at the expense of other freedoms.<sup>192</sup>

Smart contracts, according to this line of thought, are like specific performance on steroids and without the state's coercive machinery. Smart contracts make it the case that promisors will do precisely what they promise, radically strengthening promises. If this is the point of judicial contract enforcement, then it looks like smart contracts offer a superior technology, and smart contracts would leave judicial enforcement essentially obsolete.

Of course, there is room for concern within this picture of contract law as enforcing promises. First, one might suggest that smart contracts, by making performance inevitable, are no longer promises at all.<sup>193</sup> If so, smart contracts would not reinforce the practice of promising. Whereas contract law supports promising by giving promisors legal reasons to perform, smart contracts do away with the need for reasons altogether, and fail to support the moral agency involved in promising. Pragmatically, it may not be obvious why we should value promising, apart from the reliable commitments that promising enables.<sup>194</sup> But, assuming we should value promising for other reasons, then smart contracts highlight the fact that contract law

---

192. One reason to disfavor specific performance, even while recognizing that it would be preferable in terms of accurately corresponding with the underlying moral commitment, is that the coercion involved with implementing such a remedy would be too burdensome. This reason is often noted particularly with regard to personal service contracts. *See, e.g.*, 12 ARTHUR LINTON CORBIN, CORBIN ON CONTRACTS § 65.25 (Matthew Bender & Co. 2017) (1950) (“A second reason [against specific performance] is that we have a strong prejudice against any kind of involuntary personal servitude. We insist upon liberty even at the expense of broken promises.”). It is sometimes even suggested that specific performance might violate the constitutional prohibition on slavery, though the merits of this constitutional claim is questionable. *See* Nathan B. Oman, *Specific Performance and the Thirteenth Amendment*, 93 MINN. L. REV. 2020, 2025 (2009).

193. One must be cautious not to overstate the point though. Smart contracts do require a voluntary act by the contracting agent at the outset.

194. In any event, a significant further argument would be needed here. It's not transparent that a hypothetical world in which making a promise produced an unfailing compulsion to do the thing promised would be a morally impoverished world. If smart contracts make our world more like this, then they would not bolster agents' choices to keep their promises. But it's not clear why we should care about *that*.

One obvious rationale for creating reasons, as opposed to action directly, would be to respect the freedom or agency of others. I can give you reasons to raise your right hand, but I ought not simply thrust your hand upwards. But this rationale does not apply in as straightforward a way when it is one's own action, as contracting involves. If what I aim to do is to get myself to act, what I may seek is motivation rather than merely reasons.

is about creating or supporting reasons to fulfill our moral obligations, and not only about creating reliable consequences.

Second, one might think that contract law is not only about supporting promises, but about the community or state being the entity lending support. On this view, it is essential that contract law strengthens promising through a political medium. In a contract case, we collectively express our affirmation of an obligation and lend our resources to enforcing that obligation.<sup>195</sup> Smart contracts, by contrast, would strengthen promissory obligations without this state involvement. Of course, to their proponents, this is a key feature of smart contracts.<sup>196</sup> But, to others, this might be a bug. Even though smart contracts would strengthen promises, it would be problematic that this strength fails to come from the political community. Smart contracts would thus raise worries similar to those expressed toward private arbitration or penalty clauses.<sup>197</sup> That is, one might worry that something is lost simply by transferring the power away from the political community.

Leaving aside worries like these, the general point is that if the function of contract law is to strengthen moral obligations to keep promises by adding legal coercion, then smart contracts seem well suited to supplant this function. In short, if contract law is about making people keep their promises, then smart contracts look like they can do that job even better than courts.

---

195. See, e.g., Seana Valentine Shffrin, *Paternalism, Unconscionability Doctrine, and Accommodation*, 29 PHIL. & PUB. AFF. 205, 221 (2000) (“[T]he institution of contract is an institution in which the community assists people who make agreements by providing a measure of security in those agreements.”).

196. See Popper, *supra* note 49.

197. See, e.g., Owen M. Fiss, *Against Settlement*, 93 YALE L.J. 1073, 1075 (1984) (“I do not believe that settlement as a generic practice is preferable to judgment or should be institutionalized on a wholesale and indiscriminate basis. It should be treated instead as a highly problematic technique for streamlining dockets.”); Seana Valentine Shffrin, *Remedial Clauses: The Overprivatization of Private Law*, 67 HASTINGS L.J. 407, 411 (2016) (noting that remedial clauses are objectionable since they “displace the public’s role in determining the content of an important area of law and objectionably displace the judiciary’s role in providing fair and impartial judgments about the public significance of legal wrongs”). There is a significant difference for smart contracts, however. Arbitration and penalty clauses ultimately depend on judicial sanction, so that state power is ultimately at issue. Smart contracts, in contrast, do not implicate state authority in this way. So, whereas arbitration and penalty clauses necessarily implicate state power and thus arguably make the political community complicit in their results, it is harder to make such a case about smart contracts.

### B. *Contract Law as Voluntary Liability*

A second view of contract law conceives it as a method to create legal liability voluntarily, in a way that is not necessarily connected to morality or promising. According to this view, contractual obligations need not correspond to moral obligations.<sup>198</sup> Instead, contractual obligations can be fashioned where it is in the interest of parties to create them. By creating legal liability, parties can create a distinctive obligation that can serve any number of purposes, from enhancing agency<sup>199</sup> to facilitating efficient transactions.<sup>200</sup>

There are three key elements in this second view. First, contracts—as opposed to promises—involve parties agreeing to legal liability if they fail to perform. The crucial element of contract law is that certain agreements are legally binding; that is, they are subject to agreed-upon legal sanctions for breach. But whether and how any agreement is legally binding is ultimately up to the parties.<sup>201</sup> Rather than understanding legal liability as parasitic on existing moral obligations, this view sees legal liability as the elective creation of the parties involved.

Second, the legal obligations of contract reflect parties opting into liability. Insofar as parties opt into a system of legal penalties, the legal obligations describe those actions to which a legal sanction will attach.<sup>202</sup> Thus, by making it the case that a party will face a sanction

---

198. See Jody S. Kraus, *The Correspondence of Contract and Promise*, 109 COLUM. L. REV. 1603, 1617 (2009). As Professor Kraus explains:

When a correspondence account insists on enforcing a promise made by a promisor who intended it not to be legally binding, it paradoxically purports to justify a legal obligation on the ground that it enforces a moral responsibility derived entirely from the individual's free will, even though legally enforcing that obligation violates the will of the very same individual whose autonomy the moral obligation is supposed to vindicate.

*Id.*; see also Michael G. Pratt, *Contract: Not Promise*, 35 FLA. ST. U. L. REV. 801, 809–10 (2008) (“The objection to the claim that contracts are promises, which I have been pressing, exploits the fact that at least some contractual undertakings generate nothing like the moral obligation to perform that attaches to the making of a binding promise.”).

199. See, e.g., Robin Kar, *Contract as Empowerment*, 83 U. CHI. L. REV. 759, 761 (2016) (“[C]ontract law aims to empower people to use promises as tools to influence one another's actions and thereby to meet a broad range of human needs and interests.”).

200. See, e.g., Charles J. Goetz & Robert E. Scott, *Enforcing Promises: An Examination of the Basis of Contract*, 89 YALE L.J. 1261, 1266 (1980) (arguing that allowing people to bind themselves legally improves utility by shaping and encouraging promise-making activity).

201. See, e.g., Randy Barnett, *A Consent Theory of Contract*, 86 COLUM. L. REV. 269, 319 (1986) (offering a theory of contract in which “[c]ontractual enforcement . . . will usually reflect the will of the parties”).

202. On this view, it would be incoherent to imagine parties agreeing to create a legal



for failing to perform, that party thereby generates its own obligation to perform.

Third, because contracting is about parties choosing to attach legal consequences to future actions, questions of contract law should address how to determine what the parties intended, or would have chosen, *ex ante*.<sup>203</sup> The basic question is what the parties would want, perhaps subject to certain additional nuances.<sup>204</sup> A range of contract doctrines can then be explained as default rules, presumed to be what most parties would want unless they explicitly indicate otherwise.<sup>205</sup> Contract law, then, is fundamentally about enabling transactional activity, by creating a system in which one can voluntarily bind oneself through opting into flexible and predictable consequences for breach.

If this is what contract law does, then smart contracting again looks like it could supplant it. According to this second view, the fundamental purpose of contract law is allowing people to create reliable consequences, enabling them to shape their behavior. The essential feature of contracts is the communication of information about what will happen in the future.<sup>206</sup> Efficient or agency-enhancing transactions can only take place if such communication is intelligible and trusted.

Smart contracts offer the possibility of highly reliable

---

obligation to  $\phi$  and yet attaching no *ex post* legal consequences to a failure to  $\phi$ . The legal obligation necessarily and completely reflects that fact that some consequence attaches. This does not mean that obligation and the consequences are one and the same. Any given obligation might have a range of legal consequences.

203. Cf. Goetz & Scott, *supra* note 200, at 1264 (“It is important to emphasize that the proper focus here is on prospective effects, that future promising is the behavior to be influenced by the rules summarized above.”).

204. Cf. Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 *YALE L.J.* 87, 91 (1989) (“We suggest that efficient defaults would take a variety of forms that at times would diverge from the ‘what the parties would have contracted for’ principle.”).

205. See, e.g., Kraus, *supra* note 198, at 1648 (noting that “majoritarian default rules respect personal sovereignty—by maximizing the likely convergence between individuals’ promissory obligation and their subjective intent—and by increasing the benefits and reducing the costs of exercising the positive individual liberty to undertake self-imposed moral obligations”); cf. Charles J. Goetz & Robert E. Scott, *The Limits of Expanded Choice: An Analysis of the Interactions Between Express and Implied Contract Terms*, 73 *CALIF. L. REV.* 261, 263 (1985) (“Our framework departs from the conventional view that state-supplied contract clauses are means merely of reducing negotiating and other resource costs; it focuses instead on the value of implied terms as widely useful, predefined signals that reduce the incidence of certain identifiable types of formulation errors.”).

206. See Goetz & Scott, *supra* note 200, at 1267 (“[T]he promisor informs the promisee about the proposed future receipt of a benefit. The promise itself is merely the production of a piece of information about the future.”).

communication about future outcomes. This is true in two ways. First, because the agreed-upon result occurs automatically, uncertainty about performance, and about judicial recognition, disappears. A promisee no longer needs to wonder whether the promise will be kept, or whether a court will recognize the breach. Second, because the code is itself the contract, provisions are laid out in precise, operational terms by definition, to a heightened degree as compared to traditional contract language.

In a well-functioning smart contract, the contract necessarily answers interpretive questions in determinative ways. In short, if contract law exists to facilitate reliance through the ability to opt into predictable future consequences, then smart contracts seem to serve this function even more seamlessly. If contract law is a commitment mechanism, then smart contracts seem to be a superior commitment mechanism.

Again there is room for concern. Specifically, one might worry that the ex ante information costs to determine all contingencies could make smart contracting overly costly. While this is undoubtedly a significant concern, it is ultimately a practical rather than theoretical objection. If smart contracts came with an array of well-understood default rules,<sup>207</sup> that could mitigate the ex ante information costs. To the extent that they persist, it would be a contingent matter to decide in what situations the information costs outweigh the gains in certainty. Smart contracts would, at least some of the time, be a better technology than ex post contract litigation. And this reflects the fact that, on this view, smart contracts and contract law serve the same underlying function.

### *C. Contract Law as Ex Post Adjudication*

We believe that smart contracts are not, even theoretically, a substitute for contract law. Consequently, we believe that the above views about contract law's function, which appear to suggest that smart contracts could replace contract law, are unsatisfactory. These two arguments are mutually reinforcing: one can see the incommensurability of smart contracts and contract litigation by attending to the true function of contract law; and one can see the inadequacy of the above views about contract law by attending to the way in which smart contracts cannot serve the same function as

---

207. Presumably part of any smart contracting platform—and much of what competing platforms might compete over—would be supposedly majoritarian and efficient default rules.

contract law.

Both views of contract law described thus far assume an *ex ante* perspective that focuses on how contract law shapes our deliberations and motivations. That is, for both views, contract law is about giving us reasons to act. On the first view, contract law shapes our deliberation by supplementing our moral obligations with corresponding legal obligations. As such, contract law gives us an additional legal consideration in favor of keeping our promises. On the second view, contract law allows us to generate obligations that will shape our deliberations going forward, by electing to impose liability for some actions. As such, contract law creates motivations to comply, which need not correspond with our moral reasons, through the imposition of potential legal liability.

If one holds the second, motivation-creating view of contract law, then it is natural to see smart contracts as supplanting contract law. After all, why create motives for action when one can ensure the action itself?<sup>208</sup> If contract law is about facilitating our actions going forward, then the smart contract seems like an appealing innovation.

But that is not what contract law is about. Contract law does not exist to alter our reasons going forward—though it surely does that. Rather, it exists to adjudicate the justice of a situation *ex post*.<sup>209</sup> It is backward looking. Its basic function is to decide whether one party has wronged another party by failing to perform a promised action. That is, contract law is a fundamentally remedial institution, not aimed at creating new reasons to perform, but aimed at resolving disputes, taking those reasons as already given. One can see this backward-looking, remedial character in the way that contract law waits for breach, waits for an aggrieved party to bring forward a complaint, and even then rarely orders conduct.<sup>210</sup> We suggest that contract law is not about creating forward-looking reasons, because other mechanisms might serve that purpose equally or better.

---

208. The same thing might be said about creating reasons for action, *see* Shiffrin, *supra* note 189, at 749, but there are significantly more questions here. It may be that there is a value to an institution that creates reasons—causes a certain kind of normative engagement—apart from its ability to create motivation. We leave that possibility very open. But, if so, then this again highlights the inability of smart contracts to supplant contract law.

209. *Cf.* RESTATEMENT (SECOND) OF CONTRACTS ch. 16, intro. note (AM. LAW INST. 1981) (“The traditional goal of the law of contract remedies has not been compulsion of the promisor to perform his promise but compensation of the promisee for the loss resulting from [the] breach.”).

210. *See generally* Cornell, *supra* note 19 (arguing that rather than enforcing promises and their obligations, contract law enforces complaints against promissory wrongs).

A simple example can illustrate the differences between the three views. Suppose Abby promises Bob that she will pay him back the money that he is considering lending to her. By promising, Abby creates a moral obligation. She now has a special sort of reason to pay the money back. These points about obligation and reasons are true independent of the law. What might contract law add? On one view, it might add an additional obligation—a legal obligation—that corresponds with the moral obligation. So, Abby’s moral reasons to pay the money back would now be bolstered by parallel legal reasons or legal motivations. On another view, contract law might add an option for an additional liability. By promising, Abby has subjected herself to moral responsibility, and in doing so, she has created reasons to perform by opening herself up to moral sanctions. In addition, contract law allows her, if she would like, to subject herself to even more accountability—legal accountability. Thus, she could create more, or different, motivations to perform by opening herself up to a new set of sanctions. The difference between these two views is that on the first, but not the second, the legal obligations correspond with the moral obligations. But, according to both answers, contract law adds additional obligations and thus additional motivation to pay Bob back.

But an altogether different answer about what contract law adds is the view that contract law creates a forum to determine what happens if Abby does not perform.<sup>211</sup> On this view, contract law does not change anything about Abby’s obligations. Those were complete the moment that she promised—she has reason to pay the money back because she promised to pay the money back.<sup>212</sup> Contract law did not make it that case that Abby *had to* do anything; Abby herself made it the case that she *had to* do something. Contract law adds something *ex post* to deal with failure. It is not about ensuring that she performs, but about responding if she does not. Contract law enables an avenue for Bob to

---

211. This idea appears to be an element of recent civil recourse theory. *See generally* Nathan B. Oman, *Consent to Retaliation: A Civil Recourse Theory of Contractual Liability*, 96 IOWA L. REV. 529 (2011) (noting that contract law helps facilitate social welfare by holding individuals accountable without the need for recourse to private violence); Benjamin C. Zipursky, *Civil Recourse, Not Corrective Justice*, 91 GEO. L.J. 695 (2003) (arguing that contract law is a form of corrective justice designed to make aggrieved parties whole). One need not accept all aspects of current civil recourse theory to maintain that contract law is not fundamentally about the creation of reasons *ex ante*.

212. Of course, this reason may have certain special characteristics—in particular, it may be content-independent and it may be exclusionary. *See* JOSEPH RAZ, *MORALITY OF FREEDOM* 35 (1986) (“A reason is content-independent if there is no direct connection between the reason and the action for which it is a reason.”).

complain if Abby does not fulfill her obligations.

One might think that this avenue for complaint feeds back into the reasons that Abby has to perform. And, in a way, that is true. Abby does get a reason to perform from contract law—specifically, she will be liable to a complaint from Bob if she does not. But that is an indirect, independently empty reason, because it is a new reflection of the reason that she already had. It would be almost absurdly circuitous to think that contract law’s primary function was about shaping reasons in such a redundant way. It is much more straightforward to see contract law as fundamentally about adjudicating the wrongs of broken agreements, and the function of creating reason or motivation as incidental.

When one views contract law in this way, then it is apparent that smart contracting does not even purport to do what contract law does. The two have fundamentally different objectives. Smart contracting functions to ensure action. Contract law functions to recognize and remedy grievances. Smart contracts could not—even in theory—replace contract law. At best, smart contracts might reduce the need for contract litigation. But that would not mean that smart contracts serve the same function in a superior fashion.<sup>213</sup> Rather, shifting to smart contracts would mean a shift to an altogether different mode of interaction, and one not clearly superior.

#### IV. SMART CONTRACTS IN PRACTICE

If smart contracts do something fundamentally different than contract law, does that mean legal scholars can safely ignore them? Perhaps it was all just a misunderstanding, borne out of Szabo’s unfortunate choice of terminology two decades ago. If he had called his idea “intelligent agents” or “virtual vending machines,” perhaps there would be no reason to examine the legal implications further, but we believe there are still reasons. Our conclusion, that smart contracts are orthogonal to contract law, does not end the inquiry. Smart contracts will be used in situations otherwise subject to contract, and will still be nominally subject to contract law. Problems are likely to

---

213. To think otherwise would be like thinking that text messaging supplants the function of reading facial expressions insofar as the complete adoption of the former might make the latter unnecessary. Cf. Jeffrey Kluger, *We Never Talk Anymore: The Problem with Text Messaging*, TIME (Aug. 16, 2012), <http://techland.time.com/2012/08/16/we-never-talk-anymore-the-problem-with-text-messaging/> [<https://perma.cc/AGN6-AVAG>] (“Habitual texters . . . don’t get to practice the art of interpreting nonverbal visual cues.”).

arise. These in turn will produce responses with real consequences, both for the parties involved, and for the development of contract law.

Proponents of smart contracts argue they will eliminate the friction of legal disputes.<sup>214</sup> This view is overly optimistic.<sup>215</sup> While the potential benefits of smart contracts are substantial, the potential problems are significant as well. There is a Frankenstein dimension to a smart contract: an instrument that fuses something innately human, entering into and enforcing agreements, with something mechanical, derived from scientific experiments. Science fiction authors since Mary Shelley have warned of the consequences of such cyborgs.<sup>216</sup> Perhaps the benefits of smart contracts will exceed the costs. Perhaps the benefits can be magnified, or the costs minimized. We should, nonetheless, carefully assess both sides of the ledger.

Contract law is, of course, far from perfect. Yet by switching from the *ex post* adjudication of contract to the *ex ante* reduction of agreements to software code, smart contracts will in some cases merely shift problems rather than eliminate them. Smart contracts are likely to face two kinds of problems, practical and doctrinal. These difficulties will create pressure for responses. Some traditional solutions can be grafted onto the technical apparatus with limited disruption. Others, however, will involve reintroduction of law. They may even lead to greater regulatory involvement in contract.

---

214. See, e.g., TAPSCOTT & TAPSCOTT, *supra* note 8, at 109 (“[T]hrough smart contracts . . . [c]ompanies can program relationships with radical transparency . . . . And overall, like it or not, they must conduct business in a way that is considerate of the interests of other parties. The platform demands it.”); Cassano, *supra* note 93 (“Someday, these programs may replace lawyers . . . .”); Andrew Keys, *Memo from Davos: We Have a Trust Problem. Personal Responsibility and Ethereum Are the Solutions*, CONSENSYS BLOG (Jan. 19, 2017), <https://media.consensys.net/memo-from-davos-we-have-a-trust-problem-personal-responsibility-and-ethereum-are-the-solutions-19d1104946d8#c46zvkccks> [<https://perma.cc/4AQC-T4SW>] (“It is early days, and there will surely be the need of attorneys, auditors, and regulators to learn, educate and facilitate smart contracts, but the process will become much more automated, intermediaries will be removed and the cost of trust will plummet.”).

215. How widespread litigation will be is an open question. There is also the question of whether aggrieved parties in smart contract arrangements can effectively litigate. As with any transactions on a blockchain, smart contracts designate parties based on cryptographic signatures. The counterparty may be anonymous, or in a different jurisdiction.

216. See generally MARY WOLLSTONECRAFT SHELLEY, *FRANKENSTEIN, OR, THE MODERN PROMETHEUS* (1818) (highlighting the dangers that result from creating a new being). Cf. Andrea M. Matwyshyn, *Corporate Cyborgs and Technology Risks*, 11 MINN. J. L. SCI. & TECH. 573 *passim* (2010) (describing firms in the securities industry increasingly dependent on information technology as “corporate cyborgs”).

### A. Imperfections of Algorithmic Enforcement

There are significant practical limitations in replacing human enforcement of agreements with software running on the blockchain. Things simply do not always go according to plan.<sup>217</sup> Anyone who has seen an error code on their computer knows that sophisticated software-based systems are imperfect. Even if the underlying blockchain consensus mechanisms are reliable, the smart contract applications running on top of them may not be.<sup>218</sup> The failure of The DAO should be a cautionary note for smart contract developers.<sup>219</sup>

Even without bugs, there are reasons to doubt smart contracts will always operate as desired. First, they require reduction of human-readable language to machine-readable code. This limits their scope to those subjects and activities that can readily be specified.<sup>220</sup> For example, a contract to unlock my connected car upon presentation of a certain cryptographic key can easily be encoded through a programming language such as Ethereum's Solidity. The network address for the car lock, the desired key, and the action to be taken, are all subject to precise definition. At the other extreme, some contractual terms simply cannot be expressed through formal logic, because they imply human judgment. A machine has no precise way to assess whether a party used "best efforts," for example.<sup>221</sup>

---

217. See Scholz, *supra* note 33 ("First, the use of algorithms to determine terms in a contract creates the possibility for emergence, that is, results that are not and indeed could not be foreseen by the algorithm's creator. This creates situations where the entity responsible for the algorithm does not know how it works and cannot predict its behavior.").

218. Peter Vessenes, cofounder of the Bitcoin Foundation, reviewed publically available Ethereum smart contracts and estimated there were 100 errors per 1000 lines of software code. See Peter Vessenes, *Ethereum Contracts Are Going To Be Candy for Hackers*, VESSENES (May 18, 2016), <http://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/> [https://perma.cc/6ARK-9NGV]. Even for commercial software, the industry average is as high as 25 errors per 1000 lines of code. See STEVE MCCONNELL, *CODE COMPLETE: A PRACTICAL HANDBOOK OF SOFTWARE CONSTRUCTION* 521 (2d ed. 2004).

219. See *supra* notes 173–77 and accompanying text.

220. See Surden, *supra* note 15, at 682–83.

221. A computable or smart contract could be encoded with an algorithm to evaluate such imprecise terms. Human courts and juries often use proxies, formulas, or framing mechanisms to evaluate concepts such as reasonableness or best efforts. At best, however, this reduces but does not eliminate the grey areas around imprecise terms. And even when it offers a precise answer, something is lost in the process in the conversion from analog to digital.

The other way smart contracts can address non-machine-encodable terms is to reintroduce humans. The oracles that the smart contract code references to assess performance may be powered by people rather than just reporting facts in the world. Or the smart contract may incorporate an arbitrator who can resolve uncertain cases in favor of one party or the other through the multisig mechanism. See *supra* note 152 and accompanying text. At some point,

Building a computerized system able to interpret smart contracts like humans can is effectively a challenge for artificial intelligence.<sup>222</sup> And that challenge is unlikely to be solved any time soon.<sup>223</sup> Despite great advances in machine learning, computers do not have the degree of contextual, domain-specific, subtle understanding required to resolve contractual ambiguity. In this regard, smart contract platforms like Ethereum are also vastly less sophisticated than state-of-the-art artificial intelligence systems like IBM's Watson.

Even if the smart contract operates exactly as designed, it may produce suboptimal results, either in the minds of one or both parties, or as a matter of economic efficiency, because it is fixed. Sometimes, for example, nonperformance is the desirable outcome. Much has been made of the idea of efficient breach.<sup>224</sup> If a builder contracts with a carpenter to make custom woodwork for a new home, but notifies the carpenter that the home will not be built before initiation of that work, nonperformance and compensation to the carpenter may be the best result. One interpretation is that contract law is designed to facilitate such nonperformance, assuming the legal default rules for contractual remedies stood behind the parties' negotiation.<sup>225</sup> But, one need not accept the theory that the law sanctions efficient breach to appreciate that the law does not lock parties into performance.<sup>226</sup>

---

however, doing so transforms the smart contract into a conventional contract with an arbitration clause, eliminating the alleged benefits of the approach.

222. Steve Omohundro, *Cryptocurrencies, Smart Contracts, and Artificial Intelligence*, 1 AI MATTERS 19, 20 (2014), [http://delivery.acm.org/10.1145/2690000/2685334/p19-omohundro.pdf?ip=152.3.34.48&id=2685334&acc=ACTIVE%20SERVICE&key=7777116298C9657D%2E18C4EEC63BFE39A6%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=814801535&CF\\_TOKEN=37250381&\\_\\_acm\\_\\_=1506721336\\_f72d6efe11d8ca2344c4f38501c0dec5](http://delivery.acm.org/10.1145/2690000/2685334/p19-omohundro.pdf?ip=152.3.34.48&id=2685334&acc=ACTIVE%20SERVICE&key=7777116298C9657D%2E18C4EEC63BFE39A6%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=814801535&CF_TOKEN=37250381&__acm__=1506721336_f72d6efe11d8ca2344c4f38501c0dec5) [<https://perma.cc/T46Y-QCKH>].

223. "The conventional view has been that the automation of contract monitoring or compliance is beyond the capability of contemporary technology." Surden, *supra* note 15, at 632 (citing ENRICO FRANCESCONI, SIMONETTA MONTEMAGNI & WIM PETERS, SEMANTIC PROCESSING OF LEGAL TEXTS: WHERE THE LANGUAGE OF LAW MEETS THE LAW OF LANGUAGE 60–62 (2010)); Symposium, *Legal Reasoning and Artificial Intelligence: How Computers Think Like Lawyers*, 8 U. CHI. L. SCH. ROUNDTABLE 1, 19 (2001).

224. See, e.g., RICHARD A. POSNER, *ECONOMIC ANALYSIS OF LAW* 13–14 (1998); Robert L. Birmingham, *Breach of Contract, Damage Measures, and Economic Efficiency*, 24 RUTGERS L. REV. 273, 284 (1970) ("Repudiation of obligations should be encouraged where the promisor is able to profit from his default after placing his promisee in as good a position as he would have occupied had performance been rendered.").

225. See Steven Shavell, *Is Breach of Contract Immoral?*, 56 EMORY L.J. 439, 452 (2006) ("[B]reach could be immoral or moral. To know which is the case, we have to inspect the reasons for breach and the knowledge of the party committing breach.").

226. See Cornell, *supra* note 19, at 1175 ("Contract law does not offer a norm against breach of contract. This is not—as the theory of efficient breach would suggest—because contract law



The general lesson is that facts may change between the ex ante specification of contract rights and the ex post adjudication of legal effects. Parties to smart contracts can try to hedge against such changes by incorporating qualifying language or *force majeure* clauses, but those kinds of imprecise terms are difficult to specify in computer code. In other cases, parties may wish to advantageously alter a contract prior to performance. Under standard contract law, such modifications are unproblematic.<sup>227</sup> For smart contracts, such modifications pose a difficulty. Upon agreement, a smart contract is locked in place and secured by pledged cryptocurrency. To enable an intermediate step before execution, the smart contract code would need to incorporate the possibility of modification explicitly. As a technical matter, this would increase the complexity of the process. It would also introduce the kinds of difficulties already described about how to express complex ideas in code, like when and how parties can modify the set terms of a smart contract.

As the literature on relational contracts recognizes, contracts are often more than a one-time interaction between parties, followed by performance or judicial resolution of a dispute.<sup>228</sup> Instead, contracts are elements of ongoing relationships.<sup>229</sup> Both the parties and the courts view the contract in light of social and relational norms. Ex ante, parties to a relational contract must anticipate later renegotiation, and ex post, courts must determine how to fill gaps in the agreed-upon contract.<sup>230</sup> Smart contracts attempt to atomize the contractual process. They formally strip away the time dimension of interactions between the parties, and the uncertainties of future judicial resolution. Yet, smart contracts bind real people, who have real relationships, and their performance unfolds over time. This makes it impossible to avoid some of the messiness that attends traditional contracts.

### B. Doctrinal Concerns

Contract law developed over centuries to account for situations that arise in the execution of agreements. Through the inductive

---

judges breach of contract permissible when the costs are high enough. Contract law simply does not determine permissibility.”).

227. See RESTATEMENT (SECOND) OF CONTRACTS § 89 (AM. LAW INST. 1981).

228. See Ian R. Macneil, *Contracts: Adjustment of Long-Term Economic Relations Under Classical, Neoclassical, and Relational Contract Law*, 72 NW. U. L. REV. 854, 900–01 (1978).

229. See, e.g., Macauley, *supra* note 91.

230. See Eric A. Posner, *A Theory of Contract Law Under Conditions of Radical Judicial Error*, 94 NW. U. L. REV. 749, 751 (2000).

process of the common law, courts evolved solutions to novel problems. Upon closer examination, many of these rules are in tension with smart contracts' mechanism of automatic, irrevocable enforcement.

At a basic level, a smart contract can meet the legal requirements for a valid and enforceable common law contract: offer, acceptance, consideration, capacity, and legality.<sup>231</sup> But a host of potential problems lurk beneath the surface. At virtually every turn, smart contracts might operate in ways contrary to legal contracts. That is, although smart contracts may be legal contracts, they may also fall victim to almost every legal deficiency. Nothing in a smart contract ensures a true meeting of the minds; nothing ensures consideration; and so on. Below, we describe a number of ways that smart contracts might operate problematically, and contrary to the law of contracts.<sup>232</sup>

1. *Problems with Meeting of the Minds.* A smart contract is computer code representing an agreement between two or more parties, so one question might be whether it truly represents a meeting of the minds. Computers, after all, do not have minds, at least not outside the realm of science fiction. But this objection is quickly overcome. In modern contract law, offer and acceptance are evaluated objectively;<sup>233</sup> that is, we allow evidence that both parties intend to be bound, and discard evidence about indicia of internal mental states. The fact that parties submit their cryptographic private keys to commit their resources to the smart contract is proof of such an intent.

The parties' mutual intent to be bound does not, however, prove a meeting of the minds about the specific contractual provisions. The doctrine of mutual mistake excuses performance when both parties were mistaken about an essential fact.<sup>234</sup> If the smart contract refers to cotton delivered by the ship *Peerless* but there are two—or

---

231. See, e.g., *Cohn v. Fisher*, 287 A.2d 222, 224 (N.J. Super. Ct. Law Div. 1972) ("The essentials of a valid contract are: mutual assent, consideration, legality of object, capacity of the parties and formality of memorialization."); RESTATEMENT (SECOND) OF CONTRACTS §§ 12, 17, 71, 178–79 (AM. LAW INST. 1981).

232. In all the cases below, it may be possible to write exceptions into the smart contract, or into the basic code of the underlying blockchain platform, to address these situations. See *infra* Part IV.C.1. Such mechanisms are likely to be imperfect, however, and will compromise the efficiency of fully automated smart contracts. They will not automatically apply to every smart contract like a common law doctrine or statutory provision in conventional contract law.

233. See *supra* note 134 and accompanying text.

234. See RESTATEMENT (SECOND) OF CONTRACTS §§ 20(1) & illus. 2, 152 (AM. LAW INST. 1981).

seventeen—ships of that name, standard contract law can hold the agreement unenforceable.<sup>235</sup> But the smart contract would go ahead and execute.<sup>236</sup> In a unilateral contract, the mistake might not even need to be mutual for a court to rescind it.<sup>237</sup> In other words, there might be an executable smart contract that does not satisfy the legal conditions for mutual assent. This is because even seemingly *ex ante* elements of contract law, like assent, actually turn on how matters look *ex post*.

The basic problem here is that smart contracts are not really smart, at least not in the way that contract law is smart. Smart contracts are not smart enough to adjust as events unfold. Even beyond mistakes, parties may not anticipate the exact scenario that arises at the time of performance. Most contracts are incomplete, in the sense that they do not specify an outcome for every possible state of the world.<sup>238</sup> Courts can fill in the blanks when the contractual expression of the parties' intent is unclear. With a smart contract, this approach is foreclosed.

A second problem related to meeting of the minds arises when the contract itself is clear, but does not represent the intent of the parties, for example, if a party enters into an agreement due to fraud or duress. In such a situation, performance may be excused.<sup>239</sup> The contract itself is valid; it is simply not enforceable. Yet, the distinction between validity and enforceability is precisely the one that smart contracts elide.

A smart contract is valid if it is accepted as part of the consensus process on the blockchain ledger. Once that happens, it is ineluctably enforced, even if fraudulently induced. The blockchain does not have

---

235. See *Raffles v. Wichelhaus*, 159 Eng. Rep. 375, 376 (Ex. 1864). For the fact that there were at least eleven ships called *Peerless*; see A. W. Brian Simpson, *Contracts for Cotton to Arrive: The Case of the Two Ships Peerless*, 11 CARDOZO L. REV. 287, 295 (1989).

236. Probably the smart contract would use whichever *Peerless* arrived first. If a multisig arbitration arrangement were built into the smart contract, the arbitrator could choose one option. However, the arbitrator would not have the ability, absent a specific contractual provision, to return the funds to both parties and recreate the *ex ante* status quo.

237. See, e.g., *Conduit & Found. Corp. v. Atlantic City*, 64 A.2d 382, 385 (N.J. Super. Ct. Ch. Div. 1949) (“Quite plainly, this is a unilateral mistake in a contract for which equity may, under certain circumstances, grant relief by way of rescission.”); *Chicago, St. Paul, Minneapolis & Omaha R.R. v. Washburn Land Co.*, 161 N.W. 358, 361 (Wis. 1917) (“[E]quity will grant relief by rescission in proper cases for the mistake of one party as readily as for mutual mistake, where it is shown that it would be contrary to equity and against conscience to allow the enforcement of the contract.”).

238. See Oliver D. Hart, *Incomplete Contracts and the Theory of the Firm*, 4 J.L. ECON. & ORG. 119, 123 (1998).

239. See RESTATEMENT (SECOND) OF CONTRACTS §§ 162, 175 (AM. LAW INST. 1981).

any context regarding *why* parties provide private keys to authorize a smart contract, only that they did. And no one can ask an arbiter to excuse performance because she signed with a gun to her head, because there is no arbiter. The arbiters are the computers operating the blockchain, and they only listen to the code of the smart contracts themselves.

As a practical matter, furthermore, the plaintiff in such a scenario would have difficulty asserting an affirmative cause of action. Duress itself is not a tort. And fraud is significantly different as a cause of action than as an affirmative defense.<sup>240</sup> The most effective recourse for someone improperly induced to enter in a smart contract would likely be to sue for restitution of the ill-gotten gains, after the smart contract executes.

2. *Problems with Consideration.* Similar problems arise with consideration, another basic requirement for an enforceable contract. Consideration distinguishes contracts from unenforceable gifts.<sup>241</sup> All promises may create moral duties, but not all promises create legal obligations. For smart contracts, there is no test for consideration. A typical smart contract involves some consideration that induces the reciprocal promise. However, there is nothing stopping someone from encoding a gift promise to the blockchain. Such a promise would execute irrevocably, in the same manner as any other smart contract. The rest of consideration doctrine, like the distinction between adequacy and sufficiency, similarly goes by the wayside when there is no way to test enforceability before execution.<sup>242</sup>

The absence of consideration from smart contracts sheds further light on how they differ from legal contracts. Consideration doctrine supports the view that contract law exists to provide remedies for

---

240. See RESTATEMENT (SECOND) OF CONTRACTS ch. 7, topic 1, intro. note (AM. LAW INST. 1981) (“Because tort law imposes liability in damages for misrepresentation . . . the requirements imposed by contract law are in some instances less stringent. Notably, under tort law a misrepresentation does not give rise to liability for fraudulent misrepresentation unless it is both fraudulent and material, while under contract law a misrepresentation may make a contract voidable if it is either.”).

241. See JOSEPH M. PERILLO & JOHN D. CALAMARI, CALAMARI AND PERILLO ON CONTRACTS § 4.1 (6th ed. 2009); Lon L. Fuller, *Consideration and Form*, 41 COLUM. L. REV. 799, 815 (1941).

242. As another example, the preexisting duty rule in contract law rejects modifications which lack independent consideration. See *Lingenfelder v. Wainwright Brewery Co.*, 15 S.W. 844, 848 (1891); RESTATEMENT (SECOND) OF CONTRACTS § 73 (AM LAW INST. 1981). If a smart contract does specify the opportunity for mutual modification, it need not incorporate a consideration requirement when doing so.

breach, and not to generate ex ante obligations.<sup>243</sup> If the point of contract were to enforce promises, or to allow parties to advert to liability voluntarily, contract law ought to allow them to make binding gift promises. But from its ex post vantage point, contract law can distinguish unenforceable gifts and mutual legal obligations. By contrast, smart contracts load all the effort into the ex ante specification of contractual terms.

3. *Problems with Capacity.* The issues with legal capacity are somewhat different. Here, the question is not what the contract includes, but who it binds. Those without legal capacity, including children, people with significant mental impairments, and the excessively intoxicated, are excused from contractual performance.<sup>244</sup> As with consideration, smart contracts have no means to test for capacity. There is no legal limitation on minors having private encryption keys or owning Bitcoins, as they are currently restricted from having credit cards or accounts on payment services like PayPal.<sup>245</sup> And if someone digitally signs a smart contract while dead drunk, or another person exploits those circumstances to get them that person do so, there is no future opportunity for subjective evaluation by the other party.

The absence of a capacity test raises a deeper set of issues for smart contracts. The parties to a smart contract, at a technical level, are not people. They are cryptographic private keys. The secret private key represents the individual, based on a mathematical relationship with the associated public key. It is virtually impossible for someone who does not possess the private key to generate a valid digital signature that matches a given public key. This allows cryptographic keys to form the basis for digital identity systems.<sup>246</sup> Identity, however, is a rich

---

243. See *supra* Part III.C.

244. See RESTATEMENT (SECOND) OF CONTRACTS § 12 (AM. LAW INST. 1981). As with meeting of the minds, this is an objective test. See *id.* § 12(1) (“Capacity to contract may be partial and its existence in respect of a particular transaction may depend upon the nature of the transaction or upon other circumstances.”).

245. See Sean Williams, *Americans’ Average Credit Score Is Rising—How Does Yours Compare?*, NEWSWEEK (Dec. 4, 2016, 8:00 AM), <http://www.newsweek.com/americans-average-credit-score-rising-527641> [<https://perma.cc/3AVE-HBEU>] (noting that the CARD Act of 2009 prohibited those under 21 from obtaining credit cards without a parent cosigning or evidence of sufficient income to pay debts); PAYPAL, USER AGREEMENT FOR PAYPAL SERVICES § 1.2, <https://www.paypal.com/ga/webapps/mpp/ua/useragreement-full> [<https://perma.cc/75M2-GGXN>] (“To be eligible to use the PayPal Services, you must be at least 18 years old . . .”).

246. See L. Jean Camp, *Digital Identity*, IEEE TECH. & SOC’Y, Fall 2004, at 34, 40.

concept, and requires layering various capabilities for authentication, access, and more.<sup>247</sup> Moreover, even if a key uniquely belongs to an individual, the person and the key are not the same. An individual may possess many digital identities, backed by different private keys. The key may be linked to personally identifiable information that points to the specific individual. On the other hand, the key may designate a persistent digital identity hiding the associated real-world person, “pseudonymity,” or, it may give no information at all about identity, “anonymity.”

It may not be right, then, to say that smart contracts are agreements between people. In the case of the computable or data-oriented contract, the negotiation and specification of an agreement may be left entirely to machines.<sup>248</sup> But there, it is generally easy to view the computers as agents for their human programmers, who specify the conditions under which the computers can contract. The relevant practical difficulties, are not so different from those which agency law has addressed for centuries. With a smart contract, however, the connection between the humans and the agreement becomes more attenuated. The power of execution and enforcement is given over entirely to machines. The humans no longer have the capacity, in the colloquial sense, to avoid performance of the agreement. Perhaps they likewise do not have the capacity, in the legal sense, to perform it.

This analysis connects with the conclusion above that smart contracts are not promises, even if they are contracts.<sup>249</sup> That may be easy to accept conceptually, but as the foregoing discussion shows, things start to unravel when viewed doctrinally. Law bakes in assumptions about the human nature of contract. It may not be difficult as a thought experiment to imagine a contract that does not meet contract law’s doctrinal specifications. However, once one dives into the analytical problems of contract law, the difficulties quickly multiply. This illustrates why smart contracts could not supplant contract law.

4. *Problems with Legality.* Perhaps tautologically, a legally enforceable contract cannot effectuate an illegal purpose. Smart contracts, however, are not enforced by the legal system. Imagine, for

---

247. *See id.*

248. *See supra* Part I.A.

249. *See supra* Part II.A.

example, a price-fixing conspiracy implemented through a series of smart contracts that adjust prices in lockstep.<sup>250</sup> The participants could be prosecuted under antitrust law, but the smart contracts would continue to operate. Further, there is no mechanism to stop a smart contract from implementing an unconscionable term, or a term that incorporates liquidated damages amounting to a penalty. Because the smart contract is self-executing, an action in court finding the terms unenforceable may have no practical effect; the contract will be performed regardless.

The legality test and various public policy rules hint that contract, generally considered a bastion of private law, retains a penumbra of public law. Again, this reinforces the view that contract law is an adjudicative mechanism, and is not principally concerned with reasons and obligations.<sup>251</sup> Legal adjudication is a public function, drawing on the coercive power of the state. Individuals acting together may have no problem effectuating a scheme in derogation of public policy, but as Thomas Hobbes argued, the state is granted an extraordinary monopoly on violence for the very purpose of preventing the war of all against all.<sup>252</sup>

These arguments of political theorists imagining a hypothetical state of nature become tangible with smart contracts. The hacking of The DAO illustrated the problem with contracts that have no opportunity for public oversight.<sup>253</sup> The hack was simultaneously valid as an enforceable smart contract within the software system, yet demonstrably invalid as theft in the minds of the contracting parties. If the perpetrator had exploited a bug in a conventional crowdfunding service such as Kickstarter to siphon off investors' funds, there would be no practical or legal difficulty in canceling the suspect transactions and returning the funds. Ethereum, in contrast, had no alternative to the nuclear option of the hard fork. While that may have fixed the immediate problem, the solution used a bazooka to shoot a mouse and caused significant collateral damage.

Even if a hard fork is effective, it transfers final adjudication from the institution of the courts to the polity of validation nodes.<sup>254</sup> A hard

---

250. This scenario of an algorithmic conspiracy has in fact been suggested by competition law experts. *See* ARIEL EZRACHI & MAURICE E. STUCKE, *VIRTUAL COMPETITION* 47–52 (2016).

251. *See supra* Part III.

252. *See* HOBBS, *supra* note 6.

253. *See* Popper, *supra* note 172.

254. Even if a court wished to halt execution of a smart contract such as the one through which funds were stolen from The DAO, there would not necessarily be any party to enjoin. *See supra*

fork stands or falls on whether a majority of the mining power in the blockchain network adopts it. This is not how contracts work. We do not adjudicate disputes through opinion polls or the ballot box. We grant the judge or jury authority to decide, constrained by the procedures of the legal system, the traditions of the common law, and the opportunity for legislative modification going forward. The limitations of direct democracy are familiar to anyone who has read the *Federalist Papers*.<sup>255</sup> Miners' interests may be even further removed from those of the community as a whole than "factions" in a democracy.

This is not to say that smart contracts are a threat to democratic values. One can imagine many scenarios in a world where smart contracts are prevalent, but legal analysis cannot rest entirely on imagined scenarios. We have no way of knowing how popular smart contracts will become, let alone how frequently controversies like The DAO hack will arise. What matters is that the seemingly abstract conflicts between smart contracts and basic doctrines of contract law touch deeper nerves, with potentially significant consequences. And, as in Part III, we investigate smart contracts for what they illuminate about conventional contracts.

### C. *Looking Forward*

Having established that smart contracts both clarify the purpose of contract law in theory and challenge its application in practice, we conclude with a sketch about what happens next. Any recommendations at this time are necessarily provisional. Smart contracts are so new, and their prospects are so uncertain, that firm predictions are unwise, let alone normative judgments from those predictions. However, that is no reason to ignore potential consequences while there is still time to avoid them. And given the various considerations we have discussed, it is unreasonable to assume smart contracts will be implemented seamlessly.

1. *Best Practices*. The parties entering into smart contracts are not powerless to avoid their shortcomings. Knowing they cannot rely on the judicial decisionmakers to fill gaps, one can expect parties to put more effort into contract design and drafting.<sup>256</sup> Additionally, just as

---

note 96 and accompanying text.

255. See, e.g., THE FEDERALIST NO. 10 (James Madison).

256. See Karen Eggleston, Eric A. Posner & Richard Zeckhauser, *The Design and*



transactional lawyers provide expertise in the construction of business agreements, a new class of “legal engineers” may arise to aid in the creation of smart contracts.<sup>257</sup> Parties can also employ technical mechanisms to lessen the rigidity of smart contracts. For example, giving authority to human oracles who decide whether the factual basis for performance has been met,<sup>258</sup> or employing arbitrators who resolve disputes through a multisig arrangements,<sup>259</sup> may avoid some of the draconian implications of fully self-enforcing agreements.

Already, organizations involved in the development of smart contract platforms are starting to create templates that embody best practices for smart contract drafting.<sup>260</sup> Using these templates, parties could avoid repeating mistakes in prior smart contracts, and they could draw on the expertise of industry groups carefully thinking about potential pitfalls. Smart contracting systems or, “contractware” to use Raskin’s term,<sup>261</sup> could be programmed to offer templates automatically based on the desired agreement. Default terms, for example, requiring an opportunity for mutual modification prior to execution, could be mandatory to issue a smart contract on a particular platform. Parties could consult technical auditing firms to certify the integrity of smart contract code.<sup>262</sup> Even if the platforms are not subject to any legal duties regarding the contracts they enable, they still may care about avoiding harmful outcomes due to either ignorance or malfeasance by parties.

We cannot predict how well this optimistic story will play out. Surely, technical mechanisms for improving the quality of smart

---

*Interpretation of Contracts: Why Complexity Matters*, 95 NW. U. L. REV. 91, 120 (2000) (making a similar point about parties entering into incomplete contracts with uncertainty about enforcement).

257. See Nina Kilbride, *Blockchain Legal Engineering*, MONAX BLOG (May 2, 2016), <https://monax.io/2016/05/02/blockchain-legal-engineering/> [<https://perma.cc/5RUG-VCV7>].

258. See *supra* note 118.

259. See *supra* note 152.

260. See CHRISTOPHER D. CLACK, VIRAM A. BAKSHI & LEE BRAINE, BARCLAYS BANK PLC, SMART CONTRACT TEMPLATES: FOUNDATIONS, DESIGN LANDSCAPE AND RESEARCH DIRECTIONS (Aug. 4, 2016), <https://arxiv.org/pdf/1608.00771v2.pdf> [<https://perma.cc/6FZR-NGPW>]; Ian Allison, *Barclays' Smart Contract Templates Stars in First Ever Public Demo of R3's Corda Platform*, INT’L. BUS. TIMES (Apr. 18, 2016 3:45 PM), <http://www.ibtimes.co.uk/barclays-smart-contract-templates-heralds-first-ever-public-demo-r3s-corda-platform-1555329> [<https://perma.cc/8JHG-45BY>].

261. See Raskin, *supra* note 23, at 307.

262. Such smart contract code auditing firms are already beginning to spring up. See, e.g., *About*, ZEPPELIN SOLUTIONS (2017), <https://zeppelin.solutions/about> [<https://perma.cc/85BK-Z7RJ>].

contracts will not eliminate the potential problems, any more than the ready availability of skilled lawyers prevents disputes over legal contracts.

2. *Restitution.* It would be a grave mistake to think that smart contracts will eliminate litigation. Litigation—like nature—will find a way. Parties will inevitably feel they were treated unfairly at times, and they will inevitably bring those complaints to court. The difference, however, will be the posture of the litigation. Rather than complaining parties seeking fulfillment of alleged promissory obligations, complaining parties will seek to undo or reverse completed transactions. Litigation will persist, but it will shift from claims of breach, to claims of restitution.

One might think that this effectively shifts contracts from liability rules to property rules.<sup>263</sup> That's not quite right, because one could have a smart contract that awards liability damages in a self-executing way. Rather, the difference is between *ex ante* enforcement and *ex post* adjudication. We have tried to illustrate that it is a mistake to conceive of these as simply two different forms of "enforcement."<sup>264</sup>

An effort to recover already-transferred resources is different than an effort to enforce an agreement. Thus, an action for restitution is very different than an action for breach of contract. At a minimum, the roles of the parties are reversed. In an action for breach, the nonperforming party seeks to enforce a transaction; whereas, in an action for restitution, the performing party seeks to reverse the transaction. Reversing who stands as plaintiff shifts the burdens of proof and litigation. In situations such as mutual mistake, there may be no *a priori* reason to favor one side. But when actions arise from claims of fraud, repugnance to public policy, or gifts without consideration, the balance of equities may shift in undesirable ways.

Those seeking redress for injuries suffered due to smart contracts may be forced to plead actions beyond quasi contract. To take an example highlighted earlier, both the plaintiff and the defendant can raise a claim of fraud, but the legal context is quite different. The plaintiff's claim is a tort, the defendant's claim is an affirmative defense in contract, and the legal requirements are different. Moreover, in

---

263. See Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1106–10 (1972) (distinguishing property and liability rules).

264. See *supra* Part III.

practice, such litigation may unfold quite differently if the focus shifts from the contract to the technical structures associated with it.<sup>265</sup> Because the transfer of value associated with the smart contract is tied to the parties' cryptographic private keys, the plaintiff may need to sue to force the defendant to give up that key, or perhaps computer passwords protecting it. Law enforcement agencies have done just that, when pursuing proprietors of Bitcoin exchanges promoting illegal activity like drug trafficking.<sup>266</sup> If that is the model, however, we have strayed quite far from the private law domain of contract.

3. *Regulation.* Indeed, the paradoxical result of smart contracts may be to expand the scope of government intervention into technological advancements, which has traditionally been a paradigmatic environment of private ordering. Once again, the shift from ex post adjudication to ex ante enforcement creates an inversion. Contracts free individuals to trust each others' commitments because they can rely on the power of the state to enforce them in cases of breach. Smart contracts remove the state from adjudication, but in so doing, they create pressure to reintroduce the state at the front end of the process. The only way to prevent smart contracts from facilitating illegal or disfavored conduct is to regulate them.<sup>267</sup>

It is a myth that the blockchain is inherently incompatible with regulation.<sup>268</sup> Any distributed ledger system may be more or less

---

265. By analogy, the development of autonomous vehicles has given new life to the philosophical Trolley Problem and raised the question of how one can sue a car for injuries caused by its algorithms. See John Markoff, *Should Your Driverless Car Hit a Pedestrian to Save Your Life?*, N.Y. TIMES (June 23, 2016), <https://www.nytimes.com/2016/06/24/technology/should-your-driverless-car-hit-a-pedestrian-to-save-your-life.html> [<https://perma.cc/C5DZ-26NG>] (relating autonomous vehicles to the classic Trolley Problem); Matt McFarland, *Who's Responsible When an Autonomous Car Crashes?*, CNN TECH (July 7, 2016), <http://money.cnn.com/2016/07/07/technology/tesla-liability-risk/> [<https://perma.cc/8DLM-ELXS>]. Uber required passengers of its autonomous vehicle pilot program in Pittsburgh to agree to terms of service waiving any right to sue for injuries. See Mark Harris, *Passengers in Uber's Self-Driving Cars Waived Right to Sue for Injury or Death*, GUARDIAN (Sept. 26, 2016), <https://www.theguardian.com/technology/2016/sep/26/uber-self-driving-passengers-pittsburgh-injury-death-waiver> [<https://perma.cc/85DX-XSY9>]. Whether this waiver is enforceable is another question.

266. See Jon Matonis, *Key Disclosure Laws Can Be Used to Confiscate Bitcoin Assets*, FORBES (Sept. 12, 2012, 9:50 AM), <https://www.forbes.com/sites/jonmatonis/2012/09/12/key-disclosure-laws-can-be-used-to-confiscate-bitcoin-assets/#4e414655ef54> [<https://perma.cc/3JS9-L9GE>].

267. See Raskin, *supra* note 23, at 340; cf. Scholz, *supra* note 33 (making similar arguments for regulation of algorithmic contracts).

268. See Jerry Brito, *Foreword* to PAUL ANNING ET AL., THE LAW OF BITCOIN, at xiii, xiii (Stuart Hoegner ed., 2015) ("A common misconception about Bitcoin is that it is not regulated."); Jerry Brito, *Bitcoin Remains a Tool for Freedom, Even While Going Mainstream*, REASON.COM

decentralized, and more or less anonymous, based on its technical design. Bitcoin and Ethereum are examples of “permissionless” systems that have no supervisory entity authorized to accept or reject participation in the mining network.<sup>269</sup> Other smart contract platforms, such as the Corda system for interbank transactions, only recognize trusted nodes, such as member banks.<sup>270</sup> This makes them less resistant to government intervention or private domination. A Corda smart contract could easily be subject to regulatory oversight, like the Anti-Money Laundering and Know Your Customer regulations that mandate identification of bank customers.<sup>271</sup> Even for a permissionless system, centralized intervention is not impossible; it is just very difficult and costly, as shown by the Ethereum hard fork to resolve The DAO hack.<sup>272</sup>

Perhaps a more apt parallel is the regulation of digital signatures. With the rise of e-commerce in the 1990s, it quickly became clear that digital signatures based on public-key cryptography could solidify commitments in the same manner as conventional signatures on traditional contracts.<sup>273</sup> A digital signature, however, is not really a

---

(May 19, 2014), <http://reason.com/archives/2014/05/19/bitcoin-remains-a-tool-for-freedom-even> [<https://perma.cc/AAW8-6FCR>] (“The cold logic of economies of scale tend to lead to greater centralization, and thus more regulation, and this will likely happen to Bitcoin, too.”); Wright & de Filippi, *supra* note 22, at 4 (“[T]here will be an increasing need to focus on how to regulate [blockchain technology].”). *But see* Ariel Deschapell, *Why Regulating Bitcoin Won’t Work*, COINDESK (Feb. 25, 2014, 14:00) <http://www.coindesk.com/why-regulating-bitcoin-will-not-work> [<https://perma.cc/BM4R-BXEW>] (“This is what scares governments, but the point they seem to miss, is that for better or worse, they can’t do anything about [regulating Bitcoin].”). *See generally* Werbach, *supra* note 17 (arguing that in fact, legal harmonization and regulation are essential to fulfilling the promise of the blockchain).

269. *See* Swanson, *supra* note 99 (explaining the distinction between permissioned and permissionless blockchains).

270. *See id.*; Michael del Castillo, *R3 Announces New Distribution Ledger Technology Corda*, COINDESK (Apr. 5, 2016, 10:34 PM), <http://www.coindesk.com/r3cev-blockchain-regulated-businesses/> [<https://perma.cc/4LAZ-2M2U>].

271. *See* Ian Allison, *R3 Develops Proof-of-Concept for Shared KYC Service with 10 Global Banks*, INT’L. BUS. TIMES (Nov. 10, 2016, 4:15 PM), <http://www.ibtimes.co.uk/r3-develops-proof-concept-shared-kyc-service-10-global-banks-1590908> [<https://perma.cc/7AM7-7TPP>]; Aleya Begum, *R3’s Corda Uncovered: It’s Not Blockchain*, GLOBAL TRADE REV. (Oct. 1, 2017), <http://www.gtreview.com/magazine/volume-15issue-3/r3s-corda-uncovered-not-blockchain> [<https://perma.cc/LZ7K-HMZ9>] (“Corda takes a different approach. By default, information about transactions is only shared with those parties to a transaction.”).

272. *See supra* note 173 and accompanying text.

273. *See* Tim Squitieri & Paul Davidson, *E-Signatures Seen as Big Boon to Business: Companies Expect to See Huge Savings*, USA TODAY, June 15, 2000, at 7A; John Schwartz, *E-Signatures Become Valid for Business*, N.Y. TIMES (Oct. 2, 2000), <http://www.nytimes.com/2000/10/02/business/e-signatures-become-valid-for-business.html> [<https://perma.cc/J5YK-7XDM>].

signature at all. It is a private key that generates an associated public key. Ultimately, the E-SIGN Act preempted contrary state law, and ensured that rules requiring signatures could be satisfied with their digital analogues.<sup>274</sup> The legal effects and limitations of digital signatures were therefore not defined by handwriting specialists, but by government.

Under many scenarios, regulators might interpose themselves into the workings of smart contracts. Generally speaking, these will involve regulation of the contracting software platforms or blockchain validation nodes, rather than the parties themselves. Someone knowingly entering into an illegal smart contract has still violated the law, but it will likely be easier to police the enabling systems.<sup>275</sup> The kinds of smart contracts parties can form will depend on the functionality and interfaces of the available tools. This recalls the fate of P2P file-sharing systems like Napster, which facilitated widespread copyright infringement. The Supreme Court eventually concluded that even when P2P services had no specific knowledge of or ability to prevent infringing transfers, the services were still liable if set up to induce them.<sup>276</sup> A smart contract system that facilitated copyright infringement, for example, by granting users digital rights to content without proper licenses, would likely suffer the same fate.

As noted earlier, nothing technically prevents execution of an illegal smart contract.<sup>277</sup> The infamous Silk Road online marketplace used Bitcoin payments to facilitate sales of illegal goods, but the transactions themselves used the same electronic contracting mechanisms as legitimate sites like Amazon.com or Ebay.<sup>278</sup> If smart contracts can further automate such activities, or financial crimes like money laundering, there will be pressure to prohibit intermediaries from enabling or processing them. Moreover, legal requirements, like the automatic stay in bankruptcy law, can supersede contractual obligations. Courts and legislatures may attempt to require smart

---

274. Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229, § 101.114 Stat. 464 (2000) (codified at 15 U.S.C. § 7001 (2012)); *see also* Jay M. Zitter, Annotation, *Construction and Application of Electronic Signatures in Global and National Commerce Act (E-Sign Act)*, 15 U.S.C.A. §§ 7001 to 7006, 29 A.L.R. Fed. 2d 519 (2008) (explaining that a signature may not be denied solely because it is electronic, but that acceptance of electronic signatures are not mandatory).

275. *See* Raskin, *supra* note 23, at 340 (suggesting that illegal smart contracts be subject to regulation).

276. *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 936–37 (2005).

277. *See supra* Part IV.B.4.

278. *See supra* note 100.

contracting systems to incorporate exceptions for such contexts.<sup>279</sup>

Administrative regulation of smart contracts is also a possibility. Various agencies, including the Federal Trade Commission (FTC), the Securities and Exchange Commission, and the Consumer Financial Protection Board, have authority to prevent unfair or deceptive practices. This extends to situations where companies do not intend consumer harms, but fail to take sufficient precautions against them. For example, the FTC successfully brought an enforcement action against Wyndham Hotels for inadequate information security practices, which led to losses of customer data.<sup>280</sup> One could imagine a similar action against the developers of The DAO, the Ethereum Foundation, or miners who processes its transactions, based on their failure to offer adequate safeguards for funds pledged to the crowdfunding system.<sup>281</sup> It is difficult to evaluate what this would mean in practice. The Ethereum Foundation is a Swiss nonprofit, The DAO software is an open-source project, and the miners are a changing collection of voluntary participants around the world. Imposing regulatory obligations on any of them would be problematic. Yet if significant consumer harms materialize, regulators are unlikely to walk away.

An analogous situation occurred in the early days of the commercial internet. The Digital Millennium Copyright Act of 1998<sup>282</sup> gave intermediaries immunity from liability for copyright infringement, but only if they complied with notice-and-takedown procedures when notified of infringing material.<sup>283</sup> Congress or a state legislature concerned about smart contracts running amok might grant a safe harbor to software creators, application providers, and validation node operators, but condition that safe harbor on the adoption of templates, functional limitations, and audits for executable smart contracts. Such rules could be vague or overbroad, chilling the adoption of smart contracts, or they might provide security for parties who otherwise would be disinclined to use smart contracts. At this point, the specifics are too difficult to predict with any confidence.

---

279. See Raskin, *supra* note 23, at 327–29.

280. See *F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 615 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015) (upholding the FTC's action).

281. One way to reach these parties would be to treat the smart contracts as legal agents of their creators. See Scholz, *supra* note 33.

282. Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (codified at scattered sections of 17 and 28 U.S.C.).

283. 17 U.S.C. § 512 (2012).

To some degree, this is a familiar story. Where freedom of contract stands in the way of important public policy objectives, it must give ground. That occurred most famously when the New Deal eventually broke through the *Lochner* Court's resistance to economic regulation.<sup>284</sup> Smart contracting systems offer a kind of technical due process protection from legislative or judicial interference. While they may hold the state at bay to an extent, they will not eliminate it from the picture.

### CONCLUSION

Our goal has been to analyze smart contracts from the perspective of law—and vice versa. Though there is significant evidence smart contracts will eventually enjoy widespread adoption, we make no assumptions about their technical and business trajectory. Even if smart contracts turn out to be a fad, they can help us better understand legal contracts. And if blockchain-based smart contracts fail, another technology will inevitably arise to achieve the same objectives. The very act of unpacking smart contracts may help to anticipate—and thus, to mitigate—potential difficulties.

Smart contracts are just one part of the larger trend of computerized technologies purporting to displace or replace human decisionmaking.<sup>285</sup> In areas like hiring, finance, and copyright enforcement, algorithmic systems are touted for their speed, efficiency, and reliability, unlike error-prone and potentially biased humans. Indeed, the benefits are considerable. But it quickly becomes clear that machines are prone to their own errors and biases.<sup>286</sup> Additionally, the introduction of algorithmic systems into historically judgment-laden fields creates challenges for legal and practical accountability.<sup>287</sup> As a

---

284. See, e.g., *Nebbia v. New York*, 291 U.S. 502, 523 (1934) (upholding government price regulation on the grounds that “neither property rights nor contract rights are absolute; for government cannot exist if the citizen may at will use his property to the detriment of his fellows, or exercise his freedom of contract to work them harm”).

285. See generally ANDREW MCAFEE & ERIK BRYNJOLFSSON, *RACE AGAINST THE MACHINE* (2011) (detailing the replacement of workers by computers).

286. See generally FRANK PASQUALE, *THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION* (2015) (arguing that powerful economic actors use “black box” computer algorithms to expand their power, often unfairly); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016) (describing how machine learning algorithms can produce discriminatory outcomes).

287. See generally PASQUALE, *supra* note 286; Maayan Perel & Niva Elkin-Koren, *Accountability in Algorithmic Copyright Enforcement*, 19 STAN. TECH. L. REV. 473 (2016) (examining the difficulties of enforcing copyrights through online intermediaries and proposing a

result, both legal scholars and computer scientists are developing techniques to promote fairness and transparency in these decisions.<sup>288</sup> A similar dynamic can be expected for smart contracts.

Contract law is nothing if not resilient. We have little doubt it will survive the onslaught from smart contracts, if indeed that is what is happening. However, contract law may learn something about itself from its new challenger.

---

new accountability framework).

288. See Barocas & Selbst, *supra* note 286, at 675; Nicholas Diakopoulos, *Accountability in Algorithmic Decision Making*, 59 COMM. OF THE ACM 56, 62 (2016); Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 637–38 (2017); Michael Feldman et al., *Certifying and Removing Disparate Impact*, in 21 PROC. ACM SIGKDD CONF. ON KNOWLEDGE DISCOVERY & DATA MINING 259 *passim* (2015), [https://ww3.haverford.edu/computerscience/faculty/sorelle/papers/kdd\\_disparate\\_impact.pdf](https://ww3.haverford.edu/computerscience/faculty/sorelle/papers/kdd_disparate_impact.pdf) [<https://perma.cc/7GSG-5BAJ>].



# EIC 3600 Search Report

<b>Requester</b>	Name: <u>Holly John H</u> Organization: <b>TC 3600</b> Art Unit: <b>3696</b> Employee Number: <b>84035</b> Office Location: <b>KNX-2D65</b>
<b>Case Serial Number:</b>	17983311
<b>Access Search Log Number:</b>	704483

<b>Searcher:</b>	Sylvia Keys
<b>Location:</b>	EIC 3600, Knox 4B68
<b>Phone:</b>	571-272-3534
<b>Email:</b>	sylvia.keys@uspto.gov
<b>Date Completed:</b>	6/12/2023

## This search report contains the following content:

- **Search Histories**

Keyword/synonym strings and search strategies used by the EIC Searcher in completing the prior art search are included. The search history for each database or resource utilized appears at the top of each database/resource section, indicated by the database/resource section headings.

- **Search Results**

Only on-topic results are included in the search report. On-topic results include all references found that are related to the art area being searched. These references may not necessarily be useful for a rejection or other office action, but are included for the Examiner's review. Off-topic, unrelated, or irrelevant search results ("false drops" or "false hits") were removed by the Searcher. Off-topic results include all references that are unrelated to the art area being searched.

If you have any questions about this search, or about how to interpret this search report, please do not hesitate to contact the Searcher using the contact information listed above.

If you need assistance retrieving the full text of any of the references contained in this report, please contact the Searcher listed above, or the EIC 3600 Reference Desk at 571-272-3488 (x23488) or [STIC-EIC3600@uspto.gov](mailto:STIC-EIC3600@uspto.gov).

Thank you for using the EIC, and we look forward to your next search!

# Potential References of Interest

• □ 2

## SPEED QUEEN

**American Coin-Op 41.2:** 18. Crain Communications, Inc. (Feb 2000)

... offer easy activation with push-to-**start** controls, the company says.

With ... and cycle selections while auditing **machine** operation. When purchased with the ... with factory-installed card readers for **cashless operation**. The CardMate Plus System ...

• □ 5

## Multihousing equipment gets added technology. (Product News)

**American Coin-Op 42.12:** 8(1). Crain Communications, Inc. (Dec 2001)

... NetMaster(TM) System, offering customer convenience, **cashless operation** and collection control to multihousing ... money is not used to **start** the **machines**. Cards increase customer loyalty ...

□ 12

## Cash Now **initiates** new program that can boost revenues at small businesses

**PR Newswire:** 1. New York: PR Newswire Association LLC. (Sep 14, 2005)

... Since it is an entirely **cashless operation**, there is no need ... be used at any ATM **machine** or at any store that ...

# Dialog – NPL and Inventor(s)

## • Search Strategy

- **Databases:** ABI/INFORM® Professional Advanced, Abstracts in New Technology & Engineering, AdisInsight: Drugs, AdisInsight: Trials, Adis Pharmacoeconomics & Outcomes News, AGRICOLA, AGRIS, Allied & Complementary Medicine™, Analytical Abstracts, APA PsycInfo®, Aqualine, Aquatic Science & Fisheries Abstracts (ASFA), Australian Education Index, BIOSIS® Toxicology, BIOSIS Previews®, British Library Inside Conferences, British Nursing Index, Business & Industry, CAB ABSTRACTS, Chemical Business Newsbase, Chemical Engineering & Biotechnology Abstracts, Chemical Safety Newsbase, Civil Engineering Abstracts, Current Contents® Search, DH-DATA: Health Administration, Medical Toxicology & Environmental Health, DIOGENES® FDA Regulatory Updates, Drug Information Fulltext, Earthquake Engineering Abstracts, Ei Compendex®, Embase®, Embase® French Local Literature, EMCare®, ESPICOM Pharmaceutical & Medical Device News, FDAnews, FLUIDEX (Fluid Engineering Abstracts), Foodline®: MARKET, Foodline®: PRODUCT, Foodline®: SCIENCE, FSTA®, Gale Group Computer Database™, Gale Group Health Periodicals Database, Gale Group New Product Announcements / Plus®, Gale Group Newsletter Database™, Gale Group PharmaBiomed Business Journals, Gale Group PROMT®, Gale Group Trade & Industry Database™, GEOBASE™, GeoRef, HSELINE: Health and Safety, ICONDA - International Construction Database, IMS Company Profiles, IMS New Product Focus, IMS Pharma Trademarks, IMS R&D Focus, IMS R&D Focus Drug News, Inspec®, International Pharmaceutical Abstracts, Jane's Defense & Aerospace News, King's Fund,

KOSMET: Cosmetic Science, Lancet Titles, Mechanical & Transportation Engineering Abstracts, MEDLINE®, Meteorological & Geostrophysical Abstracts, New England Journal of Medicine, NTIS: National Technical Information Service, Oceanic Abstracts, PAIS International, Paperbase, PAPERCHEM, ProQuest Advanced Tech & Aerospace Professional, ProQuest Biological & Health Science Professional, ProQuest Environmental Science Professional, ProQuest Materials Research Professional, ProQuest Newsstand Professional, ProQuest Technology Research Professional, Prouis Science Daily Essentials, Prouis Science Drug Data Report, Prouis Science Drugs Of The Future™, Registry of Toxic Effects of Chemical Substances (RTECS®), SciSearch®: a Cited Reference Science Database, Social SciSearch®, ToxFile®, Transport Research International Documentation, TULSA™ (Petroleum Abstracts), UBM Computer Full Text, Weldasearch®, Zoological Record

Set#	Searched for	Results
S1	machine\$1 or "vending machine\$1"	25387792*
S2	"parking meter\$1" or "parking metre\$1" or "toll booth\$1" or "video gaming console\$1" or "offline payment operated machine\$1"	204435*
S3	(s1 or s2) and unattended	47167*
S4	(s1 or s2) and cashless	46105*
S5	"coin receiving switch\$2"	3°
S6	"electric pulse\$1"	44569*
S7	"pulse information" or "pulse data"	8783*
S8	(s6 or s7) and (provide\$1 or providing)	20347*
S9	(s6 or s7) and (determin* or assess*)	15398*
S10	option\$1 or choice\$1	67674018*
S11	s10 and (remote\$4 or faraway or distant or far or "far off") and (configuration or configured)	875137*
S12	"analog signal\$1"	104007*
S13	s12 and (emulat\$4 or imitate\$1 or mimic or mirror)	5508*
S14	("signal sequenc\$3") and (count or amplitude or shape or interval)	13779*
S15	s14 and ("pulse information")	7°
S16	s14 and (issue\$1 or issuing or issuance)	3347°
S17	"cashless operation"	193°
S18	s17 and (initiate\$1 or initiating or initiation or start\$1 or starting)	80°
S19	au((patel))	953493*
S20	payrange*	413°
S21	(s3 or s4) and s5	0°
S22	(s3 or s4) and ("coin switch**")	0°
S23	(s3 or s4) and (s8 or s9)	25°
S24	s23 and s11	12°
S25	s24 and (s13 or s15 or s16 or s18)	0°
S26	(s3 or s4) and s13	35°
S27	s26 and (s15 or s16)	0°

S28	s26 and s18	0°
S29	s1 and s13	1772°
S30	s29 and (s15 or s16)	1°
S31	s29 and s18	0°
S32	s1 and s18	25°
S33	(s19 or s20) and s29	1°

□ 5

Shorter cycle times and better surface finishes

Jordan, John M; Bradbury, Johanna L. **Modern Machine Shop** 70.11: 274. Cincinnati: Gardner Business Media Inc. (Apr 1998)

... to the U-Series wire EDM **machines**, the U53K, relies on ...  
 temperature spark. These high frequency **electric pulses** can be more efficiently delivered ... amounts of material.  
 The K-generator **provides** precise voltage control, eliminating residual ...

□ 12

MPD-Model: A Distributed Multipreference-Driven Data Fusion Model and Its Application in a WSNs-Based Healthcare Monitoring System

Gong, Jibing; Cui, Li; Xiao, Kejiang; Wang, Rui. **International Journal of Distributed Sensor Networks** Abingdon: Sage Publications Ltd. (2012)

... implement feature extraction of wrist-pulse data, we propose FEA, a ...

... and reproduction in any medium, **provided** the original work is properly ...  
 large-scale historical sensed data into **machine** learning for data fusion, treats ...

□ 1

Are they too smart by half? The little shopping cards that can encode all the details of our lives. [Late Edition]

Barker, Garry. **The Age**: 6. Melbourne, Vic.: Fairfax Digital. (Sep 26, 1998)

... Asia-Pacific, believe that once we **start** using smartcards adoption will be ...  
 transactions: recharge at Automatic Teller **machines** and later through secure Internet ...  
 Clubs want to move to **cashless operation** in their bars.  
 \* Reciprocity ...

□ 2

SPEED QUEEN

**American Coin-Op** 41.2: 18. Crain Communications, Inc. (Feb 2000)

... offer easy activation with push-to-**start** controls, the company says.  
 With ... and cycle selections while auditing **machine** operation. When purchased with the ...  
 with factory-installed card readers for **cashless operation**. The CardMate Plus System ...

□ 4

Top-load washers

**American Coin-Op** 42.2: 4. Crain Communications, Inc. (Feb 2001)

... out-of-balance system ensures that the **machine** completes wash cycles without interruption. ... laundry units. This equipment provides **cashless operation**, increasing customer safety and ... maintain its lustrous appearance. The **machine's** automatic balance system) is ...

• □ 5

### Multihousing equipment gets added technology. (Product News)

**American Coin-Op** 42.12: 8(1). Crain Communications, Inc. (Dec 2001)

... NetMaster(TM) System, offering customer convenience, **cashless operation** and collection control to multihousing ... money is not used to **start** the **machines**. Cards increase customer loyalty ...

□ 7

### Top-load washers still popular with today's coin laundry users: today's **machines** designed to push efficiency to the limit. (Equipment Review)

**American Coin-Op** 44.6: 20(3). Crain Communications, Inc. (Jun 2003)

... electronic display control equipment provides **cashless operation**, increasing customer safety and ... and cycle selections while auditing **machine** operation, simply by using the MicroWand IIIE TM] the **machine** control pad or their computer ...

□ 10

### Making the cashless case: going cashless means clearing several hurdles

Partyka, Paul. **American Coin-Op** 45.10: 22(6). Crain Communications, Inc. (Oct 2004)

... if your laundry isn't a **cashless operation** you can probably name a ...

...

... if your laundry isn't a **cashless operation** you can probably name a ... time remaining in cycle or **machine** in use. "We now offer ...

□ 12

### Cash Now initiates new program that can boost revenues at small businesses

**PR Newswire**: 1. New York: PR Newswire Association LLC. (Sep 14, 2005)

... Since it is an entirely **cashless operation**, there is no need ... be used at any ATM **machine** or at any store that ...

□ 18

### Seeing both sides of the coin: operator has a mixture of coin/cashless stores

Partyka, Paul. **American Coin-Op** 51.7: 8(2). Crain Communications, Inc. (Jul 2010)

... his coin stores to a **cashless operation**. Weiboldt's reply: "Are you ... at least twice a week, **starting** out daily at 3 a.m. ...

...

... his coin stores to a **cashless operation**. Weiboldt's reply: "Are you ...



UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

24341 7590 07/26/2023
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

Table with 2 columns: EXAMINER (HAMILTON, MATTHEW L), ART UNIT (3682), PAPER NUMBER

DATE MAILED: 07/26/2023

Table with 5 columns: APPLICATION NO. (17/973,506), FILING DATE (10/25/2022), FIRST NAMED INVENTOR (Paresh K. Patel), ATTORNEY DOCKET NO. (104402-5072-US), CONFIRMATION NO. (5383)

TITLE OF INVENTION: Method and System for Asynchronous Mobile Payments for Multiple In-Person Transactions Conducted in Parallel

Table with 7 columns: APPLN. TYPE (nonprovisional), ENTITY STATUS (SMALL), ISSUE FEE DUE (\$480), PUBLICATION FEE DUE (\$0.00), PREV. PAID ISSUE FEE (\$0.00), TOTAL FEE(S) DUE (\$480), DATE DUE (10/26/2023)

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

**PART B - FEE(S) TRANSMITTAL**

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

24341                      7590                      07/26/2023  
 Morgan, Lewis & Bockius LLP (PA)  
 1400 Page Mill Road  
 Palo Alto, CA 94304-1124

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/973,506	10/25/2022	Paresh K. Patel	104402-5072-US	5383

TITLE OF INVENTION: Method and System for Asynchronous Mobile Payments for Multiple In-Person Transactions Conducted in Parallel

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0.00	\$0.00	\$480	10/26/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
HAMILTON, MATTHEW L	3682	705-071000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.
- "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively, \_\_\_\_\_ 1
- (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. \_\_\_\_\_ 2
- \_\_\_\_\_ 3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE \_\_\_\_\_ (B) RESIDENCE: (CITY and STATE OR COUNTRY) \_\_\_\_\_

Please check the appropriate assignee category or categories (will not be printed on the patent) :  Individual  Corporation or other private group entity  Government

4a. Fees submitted:  Issue Fee  Publication Fee (if required)

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

- Electronic Payment via Patent Center or EFS-Web  Enclosed check  Non-electronic payment by credit card (Attach form PTO-2038)
- The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. \_\_\_\_\_

5. Change in Entity Status (from status indicated above)

- Applicant certifying micro entity status. See 37 CFR 1.29
- Applicant asserting small entity status. See 37 CFR 1.27
- Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature \_\_\_\_\_ Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_ Registration No. \_\_\_\_\_

**Petitioner Exhibit 1002-3997**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes details for application 17/973,506 filed 10/25/2022 by Paresh K. Patel, attorney Morgan, Lewis & Bockius LLP (PA), examiner HAMILTON, MATTHEW L, art unit 3682, and date mailed 07/26/2023.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.



## OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

### Privacy Act Statement

**The Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

<b>Notice of Allowability</b>	<b>Application No.</b> 17/973,506	<b>Applicant(s)</b> Patel et al.	
	<b>Examiner</b> MATTHEW L HAMILTON	<b>Art Unit</b> 3682	<b>AIA (FITF) Status</b> Yes

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.  This communication is responsive to October 25, 2022.  
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on \_\_\_\_\_.
2.  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
3.  The allowed claim(s) is/are 1-20. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/pph/index.jsp](http://www.uspto.gov/patents/init_events/pph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).
4.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

**Certified copies:**

- a)  All      b)  Some\*      c)  None of the:
1.  Certified copies of the priority documents have been received.
  2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5.  CORRECTED DRAWINGS (as "replacement sheets") must be submitted.  
 including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
6.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |   |  |
|---|--|
| 1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                       | 5. <input type="checkbox"/> Examiner's Amendment/Comment                             |
| 2. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br>Paper No./Mail Date _____.          | 6. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| 3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material _____. | 7. <input type="checkbox"/> Other _____.   |
| 4. <input checked="" type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date. <u>20230707</u> .     |  |

/MATTHEW L HAMILTON/  
Primary Examiner, Art Unit 3682

### ***DETAILED ACTION***

This action is in response to the initial filing filed on October 25, 2022. Claim 1 was originally filed. A preliminary amendment was filed on July 12, 2023. Claim 1 was amended. Claims 2-20 were added. Claims 1-20 have been examined and is currently pending.

### ***Notice of Pre-AIA or AIA Status***

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

### ***Inventorship***

This application currently names joint inventors. In considering patentability of the claims the examiner presumes that the subject matter of the various claims was commonly owned as of the effective filing date of the claimed invention(s) absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and effective filing dates of each claim that was not commonly owned as of the effective filing date of the later invention in order for the examiner to consider the applicability of 35 U.S.C. 102(b)(2)(C) for any potential 35 U.S.C. 102(a)(2) prior art against the later invention.

### ***Allowable Subject Matter***

Claim 1-20 is allowed.

The applicant's invention discloses a mobile consumer device with a display, processor(s), and memory: identifies a merchant device in proximity to the consumer device based on broadcasted information transmitted by the first merchant device, the broadcasted information including a first identifier corresponding to the first merchant device; transmits the first identifier to a server and receives from the server an electronic communication including identification and transaction information associated with the merchant; displays the identification information, receives user selection of the merchant identification information; and in response, displays the merchant transaction information, receives supplemental user information, and transmits the supplemental transaction information to the server for completion of the transaction.

Claim 1 is allowed because no prior art in combination, fails to teach or suggest or otherwise make obvious, all the limitations comprising:

and first merchant transaction information identifying a proposed in-person transaction between the consumer device and the first merchant, wherein the first merchant transaction information includes a merchant-specified transaction amount;

displaying the first merchant transaction information;

receiving from the user of the consumer device first supplemental transaction information, wherein the first supplemental transaction information is a selection of the merchant-specified transaction amount;

Independent claim 8 and 14 are allowed based on a similar rationale. Dependent claims 2-7, 9-13, and 15-20 are allowable based on the same rationale as the claims from which they depend.

The Examiner notes the applicant's invention is directed to patentable eligible subject matter under 35 U.S.C. 101. The applicant's invention provides an improvement over past systems, the applicant's specification discloses, "Traditional electronic payment systems for in-person transactions are one-to-one such that there is one merchant and one consumer conducting one transaction at a time. The process requires a captive, exclusive interaction between the merchant and consumer, and typically neither party may disengage from the process until the payment has completed or has been cancelled." (paragraph 0008), "Additionally, other consumers who want to make a payment to the same merchant must wait until the current transaction has completed processing. Consumers interact with the merchant sequentially and wait their turn." (paragraph 0009), "This system is acceptable in traditional retail situations where one consumer is purchasing a good or service and needs the merchant to perform "check out" tasks. In such electronic payment systems, the payment transaction is first initiated by the merchant (e.g., requesting a consumer pay a certain amount). These electronic payment systems do not work well when there are multiple consumers needing to pay a single merchant at approximately the same time, or when the merchant is not able to initiate the payment process." (paragraph 0010), "Implementations described herein provide methods and systems for enabling electronic payments via a mobile device such that multiple consumers can initiate overlapping in-person payments to a single merchant at the same time, or substantially the same time. Moreover, in some implementations, the consumer has the option to send payment to a merchant without the merchant having to request payment first." (paragraph 0012), "There are numerous use cases for such a system, some of which are currently only handled by cash payments (since existing electronic payment systems do not address the need to have multiple parties sending payments to a single merchant). One example use case involves payments to a street performer, who would traditionally put out a box, hat, or an open guitar case (collectively referred to as collection box) for audience payments. As he or she is performing, any number of audience members can drop cash into

the collection box to pay the performer.” (paragraph 0013) and “Notably, the performer (or in different contexts, a merchant) is not required to initiate the payment with each consumer and does not need to stop doing what he or she is doing. A plurality of consumers can also pay the performer/merchant without needing to wait for each transaction to finish. The transaction is asynchronous as the performer/merchant need not acknowledge the transaction before the next payment and may not acknowledge the payment at all. Methods and systems described herein allow this and similar in-person payment scenarios to be handled via electronic payments managed via mobile electronic devices associated with a merchant/performer and one or more customers.” (paragraph 0014).

Jacob, K. (2007). Are mobile payments the smart cards of the aughts? Chicago Fed Letter

The article discloses the potential future of mobile payments in consumers’ lives.

### ***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Laracey et al. US Publication 20180005220 A1 Localized Identifier Broadcasts to Alert Users of Available Processes and Retrieve Online Server Data

Laracey discloses provided systems and methods for localized identifier broadcasts to alert users of available processes and retrieve online server data. A user may visit a merchant location and engage in a transaction to purchase items from a merchant at the merchant location. The merchant may wish to alert the user of various payment methods, include payments through a payment application of the user's device using a received identifier for retrieval of an online invoice with a service provider. The merchant may utilize a merchant device to broadcast a location awareness identifier to alert the user of availability of payment processes with the service provider. Additionally, once the online invoice is

generated for a transaction, the merchant device may broadcast a payment terminal request identifier that allows the user to retrieve the online invoice using data associated with the identifier and a location for the merchant.

#### Grassadonia US Patent 10410194 B1 Customized Tipping Flow

Grassadonia discloses a technology for customizing the flow of a payment transaction at a payer's mobile device, based on parameters associated with a merchant payee to which the payer is making the payment. The payee can be a business entity that conducts transactions involving tips (e.g., restaurant, professional service, etc.). The transaction flow technology involves communication between a mobile application installed on the mobile device and a remote payment service system (PSS). A list of potential payees can be displayed for selection by the payer at the mobile application. The payees can be nearby payees identified by using, e.g., BLE, Bluetooth®, Wi-Fi®, geofence, etc. Upon selection of a particular payee by the payer, the PSS identifies one or more parameters of that payee, e.g., payee type, and generates a transaction flow that includes a tipping flow corresponding to the parameters of the merchant payee.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW L HAMILTON whose telephone number is (571)270-1837. The examiner can normally be reached Monday-Thursday 9:30-5:30 pm EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Waseem Ashraf can be reached on (571)270-3948. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: <https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent-center> for more information about Patent Center and <https://www.uspto.gov/patents/docx> for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MATTHEW L HAMILTON/  
Primary Examiner, Art Unit 3682



<b><i>Examiner-Initiated Interview Summary</i></b>	<b>Application No.</b> 17/973,506	<b>Applicant(s)</b> Patel et al.		
	<b>Examiner</b> MATTHEW L HAMILTON	<b>Art Unit</b> 3682	<b>AIA (First Inventor to File) Status</b> Yes	<b>Page</b>  1 of 1

<b>All Participants</b> (applicant, applicants representative, PTO personnel)	<b>Title</b>	<b>Type</b>
MATTHEW L HAMILTON	Primary Examiner	Telephonic
Benjamin Pezzner	Attorney of Record	

**Date of Interview:** 12 July 2023

**Issues Discussed:**

**Proposed Amendment(s)**

The applicant's representative, Mr. Benjamin Pezzner filed an amended set of claims. The additional set of claims are directed to other aspects of the invention that were not claimed in the original set of claims.

**Non-statutory Double Patenting**

The examiner requested the applicant file a terminal disclaimer in light of the related patented application 16/681,673. The terminal disclaimer was filed.

/MATTHEW L HAMILTON/ Primary Examiner, Art Unit 3682	
<p><b>Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04</b></p> <p>Please further see:  MPEP 713.04  Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)  37 CFR § 1.2 Business to be transacted in writing</p>	

**Applicant recordation instructions:** It is not necessary for applicant to provide a separate record of the substance of interview.

**Examiner recordation instructions:** Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

**Notice of References Cited**

Application/Control No.  
17/973,506

Applicant(s)/Patent Under  
Reexamination  
Patel et al.

Examiner  
MATTHEW L HAMILTON

Art Unit  
3682

Page 1 of 1

**U.S. PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-10410194-B1	09-2019	Grassadonia; Brian	G06Q20/327	1/1
*	B	US-20180005220-A1	01-2018	Laracey; Kevin	G06Q20/3278	1/1
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

**FOREIGN PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

**NON-PATENT DOCUMENTS**

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Jacob, K., Are mobile payments the smart cards of the aughts?, July 2007, Chicago Fed Letter, Federal Reserve of Chicago (Year: 2007)
	V	
	W	
	X	

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

# A COMPREHENSIVE STUDY OF BLUETOOTH SIGNAL PARAMETERS FOR LOCALIZATION

A. K. M. Mahtab Hossain and Wee-Seng Soh  
Department of Electrical & Computer Engineering  
National University of Singapore  
Email: {g0500774, weeseng}@nus.edu.sg

## ABSTRACT

We provide an elaborate discussion on Bluetooth signal parameters with respect to localization, whereby we collectively designate all types of Bluetooth specification parameters that are related to signal strength – such as RSSI, Link Quality, Received and Transmit Power Level – as *Bluetooth signal parameters*. According to our analysis and experimental results, “RSSI” and “Transmit Power Level” turn out to be poor candidates for localization, while “Link Quality” has its limitations. On the other hand, “Received Power Level” correlates nicely with distance, which makes it the most desirable Bluetooth signal parameter to be used in location systems. We contend that it is vital to choose the appropriate signal parameter in Bluetooth location systems, and we expect our work to provide useful pointers in any future design of such systems. Existing systems can also benefit by adopting the appropriate Bluetooth signal parameter in their systems, and thereby, improve their location accuracy.

## I INTRODUCTION

The future ubiquitous computing environment will consist of various types of gadgets, of which many will be equipped with wireless networking capabilities. The current popularity of Bluetooth wireless protocol – due to its short-range, low power consumption, and ease of integration – makes it a strong candidate to be incorporated into these mobile devices. With ubiquity, location awareness is expected to become a basic necessity for many applications. For example, a mobile user may require location-aware services in order to find the nearest points-of-interest, or to get around an exhibition center based on multimedia-guided tours. As a result, there is a keen interest to design positioning technologies that work indoors.

The current research efforts for indoor localization systems can largely be divided into two main categories:

- Those that rely on specialized hardware (e.g., IR or RF tags, ultrasound receiver) and extensive deployment of infrastructure solely for localization purpose [1, 2].
- Those that try to build localization systems on top of existing infrastructure (e.g., Wi-Fi networks) [3–5], and thereby, eliminating the need for any special modification at both the client and the infrastructure.

Between these two categories, the latter has a brighter prospect at achieving cost-effectiveness and deployability. Since Bluetooth is increasingly becoming popular in a wide variety of devices, and that a localization system built upon Bluetooth falls

under the preferred category above, such a system would likely gain wide acceptance in the near future.

To the best of our knowledge, previous research on Bluetooth location system either provides discouraging results when considered alone, or requires the aid of additional wireless technologies [4, 5]. These unconvincing results thus far were often used to declare that Bluetooth is ill-suited for localization.

In this paper, we provide an elaborate discussion on all Bluetooth signal parameters, and discuss their potentials and pitfalls. To our knowledge, no previous work has delved into inspecting Bluetooth signal parameters in such great detail. In the remaining of this paper, we first provide in Section II an overview of these parameters, and then analyze in Section III their effects on location systems. In Section IV, we support these analyses with our experimental findings, and finally, we present in Section V the conclusions drawn, and future work.

## II OVERVIEW OF BLUETOOTH SIGNAL PARAMETERS

We use the term *Bluetooth signal parameters* to denote all the status parameters of a Bluetooth connection together with any other signal strength values made available in Bluetooth Core Specification [6]. The Host Controller Interface (HCI) provides access to three such connection status parameters, namely, Link Quality (LQ), Received Signal Strength Indicator (RSSI), and Transmit Power Level (TPL). All these status parameters require the establishment of an active Bluetooth connection in order to be measured. From Bluetooth 1.2 onwards, another signal parameter, “Inquiry Result with RSSI”, is made accessible. This is a special inquiry procedure which perceives RSSI from the responses sent by its nearby devices. To date, these are the 4 signal-related parameters made available by Bluetooth Core Specification. In the following, we briefly discuss each.

### A Link Quality (LQ)

LQ is an 8-bit unsigned integer that evaluates the perceived link quality at the receiver. It ranges from 0 to 255; the larger the value, the better the link’s state. For most Bluetooth modules, it is derived from the average bit error rate (BER) seen at the receiver, and is constantly updated as packets are received. However, the exact mapping from BER to LQ is device-specific. LQ is used mainly for adapting to changes in the link’s state, notably to support CQDDR (Channel Quality Driven Data Rate).

### B Received Signal Strength Indicator (RSSI)

RSSI is an 8-bit signed integer that denotes whether the received (RX) power level is within or above/below the Golden Receiver Power Range (GRPR), which is regarded as the ideal

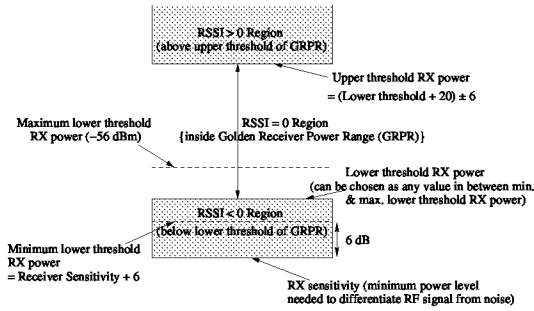


Figure 1: Relationship between GRPR and RSSI.

RX power range. Fig. 1 illustrates the relationship between GRPR and RSSI, as defined in Bluetooth specification. A positive or negative RSSI (in dB) means the RX power level is above or below the GRPR, respectively, while a zero implies that it is ideal (i.e., within GRPR). The lower and upper thresholds of GRPR are loosely bound, leaving them to be device-specific. This, in turn, affects the RSSI, since it is merely a relative parameter. In fact, its absolute accuracy is not mandated in the specification; the only requirement is to be able to indicate whether it is within, above, or below the GRPR. The RSSI status parameter of Bluetooth is particularly intended to be used for power control purpose [6]. The receiver sends “increase” or “decrease” TPL request to the transmitting side, depending on whether the perceived RSSI at its side is negative or positive, respectively.

### C Transmit Power Level (TPL)

TPL is an 8-bit signed integer which specifies the Bluetooth module’s transmit power level (in dBm). Although there are instances when a transmitter will use its device-specific default power setting to instigate or answer inquiries, its TPL may vary during a connection due to possible power control. For Class 1 devices, which have a maximum output power of +20 dBm, power control is mandatory when the TPL is between +4 and +20 dBm. In Bluetooth specification, power control is optional for TPL under +4 dBm. Therefore, Class 2 (maximum output power +4 dBm) and Class 3 (maximum output power 0 dBm) devices need not support power control, although their manufacturers may choose to implement it.

### D Inquiry Result with RSSI

“Inquiry Result with RSSI” works in a similar manner as a typical inquiry. In addition to the other parameters (e.g., Bluetooth device address, clock offset) generally retrieved by a normal inquiry, it also provides the RSSI value. Since it requires no active connection, the radio layer simply monitors the RX power level of the current inquiry response from a nearby device, and infers the corresponding RSSI.

## III ANALYSIS

In this section, we analyze the various signal parameters’ effects on location systems, as well as the different challenges

Table 1: LQ Conversion Algorithm of CSR Chipsets

BER, $\beta$ (%)	LQ conversion equation	LQ value, $l$
$0 \leq \beta \leq 0.1$	$l = \lfloor 255 - \frac{\beta}{0.0025} \rfloor$	$255 \geq l \geq 215$
$0.108 \leq \beta \leq 10.1$	$l = \lfloor 215 - \frac{\beta - 0.1}{0.08} \rfloor$	$214 \geq l \geq 90$
$10.74 \leq \beta \leq 67.7$	$l = \lfloor 90 - \frac{\beta - 10.1}{0.64} \rfloor$	$89 \geq l \geq 0$

posed by their inherent characteristics.

### A Effect of LQ

As previously mentioned, the mapping from BER to LQ is device-specific. For our experiments, we have chosen Ranger’s BT-2100 Bluetooth USB adapters, which use BlueCore4-ROM chips from Cambridge Silicon Radio (CSR). Table 1 shows the LQ approximation algorithm that they use. Since LQ is an 8-bit integer, it can only assume 256 different values to represent various BER conditions. From Table 1, we can see that LQ does not always decrease at the same rate when BER increases. For example, when we consider LQ between 255 and 215, each consecutive LQ value denotes an additional 0.0025% BER, whereas between 214 and 90, each consecutive value means an additional 0.08% BER. In other words, CSR chips report LQ with finer BER resolution when BER is small, but as the BER increases, the resolution becomes coarser. According to Bluetooth specification, a link is only considered workable if its BER is at most 0.1%. Therefore, it makes sense for LQ values below 215 to be mapped with a coarser BER resolution, as the link is already considered undesirable.

Prior works [4, 5] generally recorded LQ perceived by the mobile device as location fingerprints during the training phase. But we argue that devices that use chipsets from different vendors other than the one used at the mobile host during the training phase may unfortunately produce quite different LQ readings, because their LQ conversion algorithms may differ.

### B Effect of RSSI

The RSSI reported by a Bluetooth device is completely dependent on the device’s GRPR and its power control mechanism. The nominal range for GRPR of any Bluetooth device, according to Bluetooth specification, is  $20 \pm 6$  dB. We have earlier seen that RSSI is 0 when the RX power level is within GRPR. Now, let us investigate RSSI’s relationship with distance, and consequently, infer how it might affect location systems. Suppose a Bluetooth transmitter’s TPL is set to  $P_t$ . Let  $P_{d_1}$  and  $P_{d_2}$  denote the upper and lower GRPR thresholds of the intended receiver, and assume that these power levels are detected at distances  $d_1$  and  $d_2$ , respectively, from the transmitter. According to the free-space propagation model,

$$P_{d_1} \propto \frac{1}{d_1^2} \text{ and } P_{d_2} \propto \frac{1}{d_2^2}, \text{ giving } \frac{P_{d_1}}{P_{d_2}} = \frac{d_2^2}{d_1^2}. \quad (1)$$

If we consider 20 dB path loss between these two distances, which is approximately the nominal GRPR range, we get

$$10 \times \log \frac{P_{d_1}}{P_{d_2}} = 20. \quad (2)$$

Combining (1) and (2), we finally obtain

$$\frac{d_2}{d_1} = 10. \quad (3)$$

The above calculation implies that RSSI remains at 0 when the separation ranges between  $d_1$  and  $d_2$ , although they differ by a factor of 10. Hence, we may not be able to differentiate over a wide area if we rely on RSSI for localization. To aggravate the problem, Bluetooth devices may request the transmitter to perform power control, so as to keep its RX power level within GRPR. Suppose the devices choose to perform power control over a range of 20 dB (the margin may even be larger according to Bluetooth specification). If we add this quantity to the 20 dB GRPR range, it means we can no longer discriminate path losses of 40 dB. Following the same analysis as before, it can be seen that, a device only 10 cm away may not be distinguishable from one that is 10 m away. This wide range is unacceptable for indoor localization. Hence, RSSI is argued to be a poor candidate for location systems.

### C Effect of TPL

The power control feature is introduced into Bluetooth devices in order to facilitate energy conservation, and also to combat interference. The step size for power adjustments ranges between 2 and 8 dB. Upon receipt of a power control request message, the TPL is increased or decreased by a step.

Although according to specification, Class 1 devices are advised to perform power control even below  $-30$  dBm, for the convenience of analysis, we assume here that the minimum selectable power is  $-30$  dBm. In this scenario, Class 1 devices can thus vary its power over a range of 50 dB, since the maximum attainable power for Class 1 devices is  $+20$  dBm. If we consider the minimum power control step size of 2 dB, then there can be at most  $50 \div 2 = 25$  different TPL values for distinguishing unique locations, which is quite limited.

Our CSR adapters offer updated RSSI measurements once every second. Therefore, if it takes four power control steps to eventually reach a stabilized TPL for a specific location, the overhead can be as long as 4 seconds (ignoring transmission and processing delays), which contributes to the overall latency of such a location system.

### D Effect of Inquiry Result with RSSI

Every inquiry that is sent and replied by a device will be transmitted at a device-specific default power setting. As a result, the RSSI fetched through an inquiry is free from the side-effect of power control as explained earlier. Hence, the inquiry-fetched RSSI is expected to provide finer measurements than the connection-based RSSI, although it still suffers from the GRPR-related zero-RSSI problem.

The Bluetooth inquiry procedure uses 32 dedicated inquiry hop frequencies (in countries with 79 Bluetooth frequency

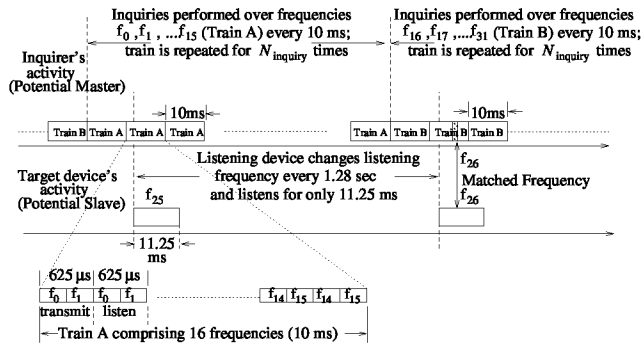


Figure 2: Potential Master's and Slave's frequency scanning during Bluetooth inquiry procedure (in countries with 79 Bluetooth frequency channels) [6].

channels) according to the inquiry hopping sequence as defined in the Bluetooth specification [6]. The inquiry-hopping rate is twice the nominal frequency-hopping rate used by ordinary connections. In other words, an inquiring device switches to a new frequency every  $312.5 \mu s$ , whereas a typical Bluetooth time slot is  $625 \mu s$  long. The inquiry hopping sequence is split into two trains, A and B, of 16 frequencies each (see Fig. 2). In one slot (i.e.,  $625 \mu s$ ), the inquiring device sequentially transmits on two different frequencies. In the following slot, it shall listen for any response to the previous two frequency hops, in the same sequence. Consequently, each train comprises 16 alternate transmitting and listening slots, and spans  $625 \mu s \times 16 = 10$  ms. According to Bluetooth specification, a single train is repeated for at least  $N_{inquiry} = 256$  times before switching to a new train. In an error-free environment, a Bluetooth device is recommended to perform at least three such switches in order to collect all responses. As a result, the whole inquiry procedure may last for  $4 \times (256 \times 10 \text{ ms}) = 10.24$  sec, which can be a major drawback if latency is a prime concern. Nevertheless, the Bluetooth specification allows some flexibility pertaining to this inquiry duration. For example, the inquirer may stop inquiry process if it has collected enough responses.

## IV EXPERIMENTS

In this section, we first describe our experimental testbed. We then elaborate on our data collection procedure, and present the results along with discussions.

### A Testbed

Our experimental testbed is located within a research laboratory. It has a dimension of  $21.6 \text{ m} \times 9.56 \text{ m}$ , an area of  $206.496 \text{ m}^2$ , and includes many small cubicles for research students. The whole experimental area is divided into an  $11 \times 6$  grid, resulting in a unit grid size of  $2.16 \text{ m} \times 1.912 \text{ m}$ . We placed three BT-2100 Class 1 Bluetooth adapters in three such grid positions to serve as APs, and connected them to nearby Pentium-based PCs. As Bluetooth APs in an actual location system will invariably be located near ceilings, we raised our Bluetooth adapters with the help of USB cables, and attached them to the roof ( $2.57 \text{ m}$  above the floor). Our mobile host,

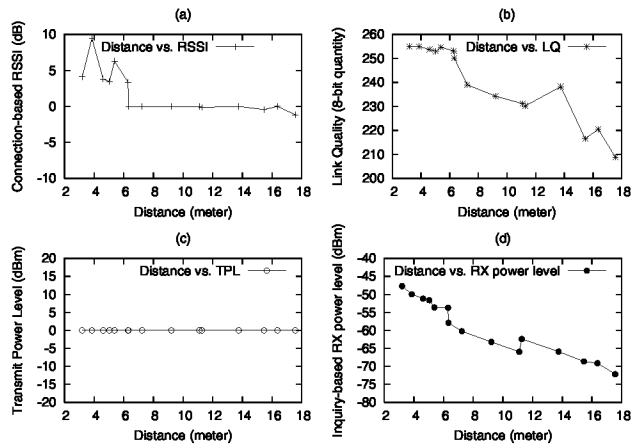


Figure 3: Relationship between various Bluetooth signal parameters & distance.

which is carried by the experimenter, is a Pentium-based Tablet PC. All the desktops (connected to the Bluetooth adapters by USB cables) together with our Tablet PC run Fedora Core 4, with the latest BlueZ protocol stack [7].

### B Data Collection, Results and Discussion

During the experiments, our mobile host is connected using “SSH” (secure shell) to the desktops controlling the Bluetooth adapters. This facilitated the experimenter to have complete control over the whole system from the mobile host. While standing at a specific grid position, the experimenter could run Bluetooth signal extractor programs at both the mobile host and any AP over the network.

We now present the results from our various experiments:

#### 1) Signal parameters’ correlation with distance

For this experiment, we carefully chose five different grid positions where we took readings from each of the 3 APs, thus resulting in 15 data points. We adopted this methodology, rather than choosing 15 distinct distances from a single AP, because we wanted to correlate distance with signals originating from APs that were placed at different locations and surroundings.

In our experiments, we discovered that the Bluetooth wireless signal strengths tend to vary quite significantly depending on the user’s orientation. Therefore, for every chosen grid position, we took 30 readings from every AP for each of the four different orientations. We then calculated the average of these 120 readings to obtain the signal parameter’s value for that particular AP at the specific grid position. Since we know the distances of all grid positions from any AP, the signal strength values are simply mapped against the corresponding distances to generate Fig. 3.

In order to acquire the connection-based status parameter readings (i.e., RSSI, LQ, and TPL), we maintained connections at the HCI level from the APs to our mobile host.

From Fig. 3, the following observations can be made:

- As anticipated in our earlier analysis, RSSI turns out to correlate poorly with distance, as shown in Fig. 3(a).

- Fig. 3(c) shows a horizontal straight line for TPL values. This is because our Class 2 adapter at the mobile host which uses Broadcom’s BCM2035 chip does not support power control feature. As a result, the TPL at the AP remained at its default value, which happens to be 0 dBm for the Bluetooth adapter used.
- From Fig. 3(b), we see that LQ correlates with distance much better than RSSI and TPL, although the LQ readings obtained at smaller distances show very little variation. Note that these readings were taken at the AP side, rather than at the mobile host side, as the LQ perceived at our mobile host was always 255 at any grid position, which is the highest possible LQ value. This is due to our Class 1 APs’ large transmit power. The measurements at the AP side, on the other hand, show variations because our mobile host uses a Class 2 adapter.
- Our BT-2100 Class 1 adapters provide absolute RX power level through inquiry, instead of the relative RSSI values as suggested by Bluetooth specification. As the parameter “Inquiry Result with RSSI” also suffers from the GRPR-related zero-RSSI problem (just like the “connection-based RSSI”), we believe that making RX power level available should augur well in terms of distance. Fig. 3(d) certainly establishes this claim since the RX power level shows the best correlation with distance, compared to the other three signal parameters.

#### 2) Effect of GRPR on RSSI

Fig. 5(a) illustrates the adverse effects of wider GRPR on the reported RSSI. From the figure, it is seen that BT-2100’s RSSI readings (GRPR  $\approx$  80 dB ) showed little variation compared to our Broadcom’s adapter, which has a narrower GRPR. Because of the combined effect of large GRPR and power control, BT-2100’s RSSI readings always remained at or above 0. On the contrary, Broadcom’s adapter gave negative RSSI values at greater distances, although we did not have many such grid positions owing to our testbed’s size.

#### 3) TPL Consideration

For this experiment, we recorded the stabilized TPL values as well as the stabilization time periods for each AP’s signal at specific grid positions using BT-2100 at the mobile host side. Fig. 4(a) indeed shows very few discrete transmit power levels, in harmony with our analysis in Section C. Moreover, the time periods required to reach these stabilized TPL values are also quite significant, as revealed in Fig. 4(b). Both these attributes make TPL a poor candidate for localization purpose.

#### 4) Effect of Varying Inquiry Time Period

In this experiment, the inquirer, which is the mobile host, is placed at a location where it can hear all 9 Bluetooth devices to be discovered. Since BlueZ’s HCI API allows us to vary the inquiry time period in increments of 1.28 sec, we varied it accordingly, and took 50 readings for each distinct inquiry time period. From Fig. 5(b), it is observed that, although the gap between the maximum and the minimum number of discovered

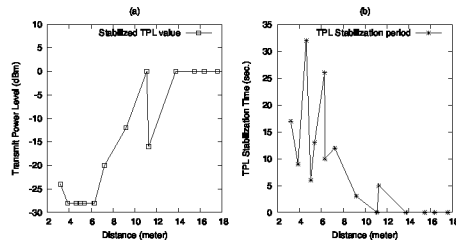


Figure 4: Stabilized TPLs & time periods to attain them.

devices can be quite large when the time periods are small, the average number of discovered devices is actually quite impressive at time period as low as 3.84 sec while the suggested inquiry time period in an error-free environment is 10.24 sec.

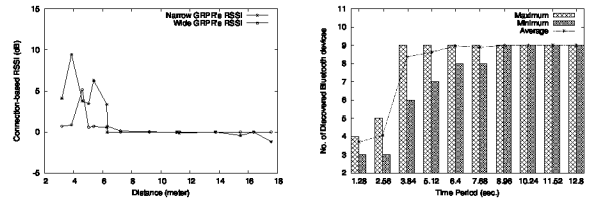
### V CONCLUSION AND FUTURE WORK

Based on our analysis and experimental results, the following conclusions can be drawn:

- Similar to previous works' verdict, we have shown RSSI's incompatibility for location systems. While previous works based their judgement solely on experimental data, we have also backed it up with proper analysis.
- To the best of our knowledge, no prior Bluetooth localization work has tried to use TPL. From our findings, we conclude that TPL is not suitable for localization.
- Through our experiments, we have shown that the LQ perceived at any location are rather sensitive to the transmitter's Bluetooth class. Therefore, problems would likely arise if LQ measurements were made at the AP side, and the mobile host's Bluetooth class is unknown. On the other hand, if LQ measurements were taken at the mobile host side, the fingerprints would then be sensitive to the BER-to-LQ mapping algorithm used by the mobile host, which is device-specific. Thus, LQ is not suitable for localization. Existing works on LQ-based localization [4, 5] have also reported poor location accuracy so far.
- Location systems that depend on inquiry-based parameters should take into account the latency incurred during the inquiry. Our experimental results show that the default time period for Bluetooth inquiry may be reduced to some extent while still providing acceptable results.
- Because of RX power level's superior correlation with distance, location systems that rely on it would likely outperform any other location systems built upon other Bluetooth signal parameters.

The major contribution of our work is a complete understanding of the Bluetooth signal parameters' issues regarding localization. We contend that it is vital to choose an appropriate signal parameter for a location system. In the following, we list some important future directions that we foresee:

- We have earlier seen that the LQ readings do not vary much at close-range distances. On the other hand, we notice that the RSSI readings tend to change significantly at



(a) Connection-based RSSI for 2 different Bluetooth adapters with different inquiry time periods (Total no. of devices = 9).

Figure 5: RSSI comparison of 2 different Bluetooth adapters and Effect of Inquiry time variation on the number of discovered devices

close-range distances as well as at distant locations, where the RX power levels are above and below the GRPR, respectively. Therefore, a hybrid location system that combines both LQ and RSSI may be a viable option.

- While the retrieval of inquiry-based signal parameters tends to induce latency to the location system, our results show that most nearby Bluetooth devices are discovered even when the inquiry time period is reduced. Therefore, more extensive analyses are needed in this regard.
- There is no additional latency in obtaining the connection-based signal parameters only if the location system already has pre-established connections to the mobile hosts. On the contrary, if a mobile host needs to be discovered and then subsequently connected when it requests for location service, it will also undergo the latency problem similar to the inquiry-based location systems. The designer of a location system needs to address these issues.
- Finally, if future Bluetooth specification decides to make RX power level available – both as a connection-based status parameter and also through inquiry, it should then instigate new possibilities for Bluetooth localization.

### REFERENCES

- [1] R. Want, A. Hopper, V. Falcão and J. Gibbons, The Active Badge Location System, *ACM Trans. on Information Systems*, Vol. 10, No. 1, pp. 91-102, Jan. 1992.
- [2] A. Ward, A. Jones and A. Hopper, A new location technique for the active office, *IEEE Personal Communications* 4(5), pp. 42-47, Oct. 1997.
- [3] P. Bahl and V. N. Padmanabhan, RADAR: An in-building RF-based user location and tracking system, *Proc. IEEE INFOCOM*, Vol. 2, pp. 775-784, Mar. 2000.
- [4] D. Pandya, R. Jain and E. Lupu, Indoor Location Using Multiple Wireless Technologies, *IEEE PIMRC*, Beijing, China, September 2003.
- [5] Y. Gwon, R. Jain and T. Kawahara, Robust Indoor Location Estimation of Stationary and Mobile Users, *Proc. IEEE INFOCOM*, Mar. 2004.
- [6] Bluetooth Special Interest Group, Bluetooth Core Specification v1.2, <https://www.bluetooth.org/spec/>.
- [7] BlueZ – Official Linux Bluetooth protocol stack, <http://www.bluez.org/>

**STATE OF THE ART**

# *In Arrival of 2 iPhones, 3 Lessons*

**By David Pogue**

Sept. 17, 2013

We can draw three lessons from the arrival of Apple's two new iPhone models, the 5C and 5S.

**LESSON 1** Apple may have set its own bar for innovation too high.

Year after year, Steve Jobs used to blow our minds with products we didn't know we wanted. Now, two years after his death, we still expect every new iPhone to clean our gutters, cook our popcorn and levitate. So when the hardware revisions are minor each year, we're disappointed.

And sure enough, after Apple showed off its two new iPhone models last week, its stock dropped. Analysts shrugged that they contain nothing "transformative." The blogger-haters had a field day.

The budget model, the new iPhone 5C, comes in five colors (\$100 for the 16-gigabyte model with a two-year contract, \$550 without). It's essentially identical to last year's iPhone 5, except that its back and sides are a single piece of plastic instead of metal and glass.

Actually, "plastic" isn't quite fair. The 5C's case is polycarbonate, lacquered like a glossy piano. Better yet, its back edges are curved for the first time since the iPhones of 2008. You can tell by touch which way it's facing in your pocket.

It's a terrific phone. The price is right. It will sell like hot cakes; the new iPhones go on sale Friday. But just sheathing last year's phone in shiny plastic isn't a stunning advance.

**LESSON 2** The smartphone is mature.

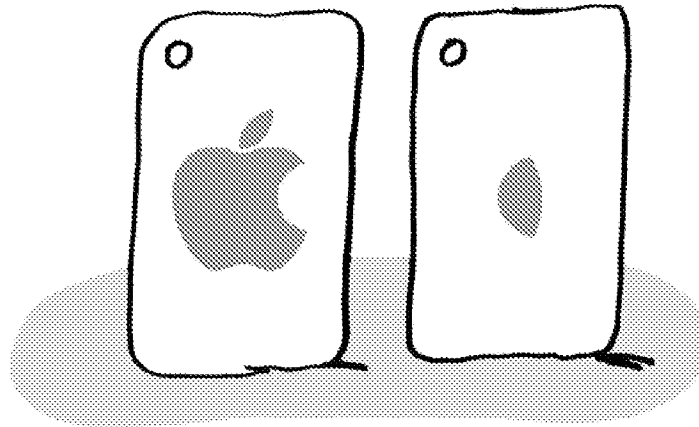
The App Store filled a huge hole. Siri voice command answered a desperate need. And high-resolution Retina displays helped compensate for the tiny screen.

But today, every phone has that stuff; the big holes have been plugged. Maybe the age of annual mega-leaps is over.



The new 5S (\$200 with contract, \$650 without) looks exactly like last year's thin and gorgeous iPhone 5. You can now get it with its brushed aluminum body in dark gray (with black glass accents), silver (white accents) or a surprisingly classy-looking gold (white accents).

Apple says the 5S's chip is twice as fast as before. Nobody was exactly complaining about the iPhone's speed before, but, sure, it's plenty quick. Since it's a 64-bit chip, Apple says the graphics in 3-D video games look especially smooth and detailed.



Stuart Goldenberg

There's also a second chip devoted to tracking motion data from the phone's compass, gyroscope and tilt sensor. Apple says this coprocessor should save battery life when you use fitness tracking apps, because it can monitor your data all day long; the main chip, which requires six times as much power, can remain asleep.

Those are both fairly invisible changes, though.

The new camera will mean more to you. Its sensor is 15 percent bigger, and the individual light-detecting pixels are bigger. Take photos side-by-side with the iPhone 5S's predecessor, and the difference is immediately obvious; lowlight pictures are far better on the new phone. Clearer, brighter, better color.

---

**SIGN UP FOR ON TECH WITH SHIRA OVIDE:** *Your guide to how technology is transforming our lives and the world.*

**Sign Up**

The 5S also has two LED flashes — one pure white, one amber — that fire simultaneously. When mixed in the right balance, their light can match the color tone of your subject (moonlight, streetlights, fluorescents, whatever). Apple says this idea is a first in both phones and cameras.

Petitioner Exhibit 1002-4015

Petitioner Kiosoft Exhibit 1005

It really works. Flash photos look much, much better. No longer will your loved ones' skin look either nuclear white or "Avatar" blue.

The 5S's camera also offers a burst mode (10 frames a second), 3X zooming during video capture, Instagram-style photo filters and truly wowing slow-motion video. (Weirdly, filtered photos and slo-mo videos don't survive the transfer to your computer, although you can send them by e-mail or text message.) Sample photos and videos accompany this column online.

The most heavily promoted feature is the 5S's fingerprint sensor, which, ingeniously, is built into the Home button. You push the Home button to wake the phone, leave your finger there another half second, and boom: you've unlocked a phone that nobody else can unlock, without the hassle of inputting the password. (And yes, a password is a hassle; half of smartphone users never bother setting one up.)

The best part is that it actually works — every single time, in my tests. It's nothing like the balky, infuriating fingerprint-reader efforts of earlier cellphones. It's genuinely awesome; the haters can go jump off a pier.

The 5S can also scan your fingerprint when you're buying books, music, apps and videos from Apple, saving you the password entry (although this, too, is buggy; Apple says a fix is due on Friday).

You can teach your iPhone 5S to recognize up to five fingerprints — all yours, yours and your spouse's, or whatever.

Apple says your fingerprint is stored only on your phone, encrypted and never transmitted or stored online. And using the fingerprint reader is optional; you can always use a regular password instead.

The sound quality of both new iPhones is excellent, whether up to your ear or filling your office with music. Apple says battery life is about 25 percent better than before; I've been getting nearly two days of moderate use on a charge.

So yes, Lesson 2 is that the speed of innovation seems to be slowing down, but don't let that depress you. Focus instead on the silver lining: you can keep your current phone longer without feeling obsolete quite so soon.

(Speaking of obsolescence: If you've held out upgrading since the iPhone 4 or 4S, remember that the new phones use Apple's new charging connector. It doesn't fit any existing charging cables, speaker docks or alarm clocks without a \$35 adapter. Grrr.)

**LESSON 3** If we're reaching a point of diminishing returns in hardware breakthroughs, the software breakthroughs are only just getting under way.

The new iPhones come with iOS 7, a redesigned operating system. You can also install it on recent iPhone, iPad and iPod Touch models.

This software looks *nothing* like the old iOS. It's all white and clean, almost barren. Its Home screen and dialogue boxes use thin fonts and a color palette of bright, light hues.

Above all, it completely abandons Apple's formerly favorite design principle, skeuomorphism, in which on-screen things depict real-world materials (lined yellow paper for Notes, leather binding for Calendar, wooden shelves for iBooks).

You might love this design, and you might loathe it. You also might get used to it. But in any case, iOS 7 is more efficient to navigate, because nothing on the screen is eye candy; everything is a button, so you spend less time hunting for things.

Furthermore, Apple did an insane amount of work on features. Some are big-ticket items like Siri, which responds faster, has a more realistic voice and understands new kinds of commands (including "Make the screen brighter" and "Turn on Bluetooth").

A supremely useful Control Center offers one-touch buttons to change important settings (thanks for the idea, Android!). AirDrop shoots pictures, maps, Web sites and other items to nearby iOS 7 gadgets, quickly and wirelessly.

You can read a full review of iOS 7 on my blog at [nytimes.com/pogue](http://nytimes.com/pogue). (A note: I have written a how-to manual to the iPhone and to iOS 7 for an independent publisher; it was neither commissioned by nor written in cooperation with Apple.)

Now, Apple's competition in the Android world is fierce and gaining; the competitors include phones that are equally beautiful (from HTC), phones that take spoken commands without your having to press a button (from Motorola) and phones in every conceivable screen size (Samsung).

But that doesn't mean that the iPhones have been *overtaken*. The iPhone's ecosystem is a deal-sweetening perk — the best apps; the best-stocked online stores for music and movies; smooth synchronizing of your calendars, addresses and even photos among Apple phones, tablets and Macs; and enough cases and accessories to reach from the landfill to the moon.

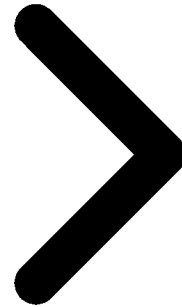
If you wanted to summarize all three of this week's lessons into a single final thesis, here it is: Apple still believes in superb design and tremendous polish. The iPhone is no longer the only smartphone that will keep you delighted for the length of your two-year contract — but it's still among the few that will.

Apple TV 4K   Eurovision 2021   NBA Playoffs   Apple Watch 3   World's largest iceberg break free in Antarctica

---



BEST



RE

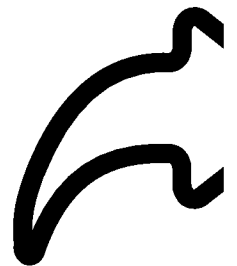
# How to use S Beam on your Samsung Galaxy S3

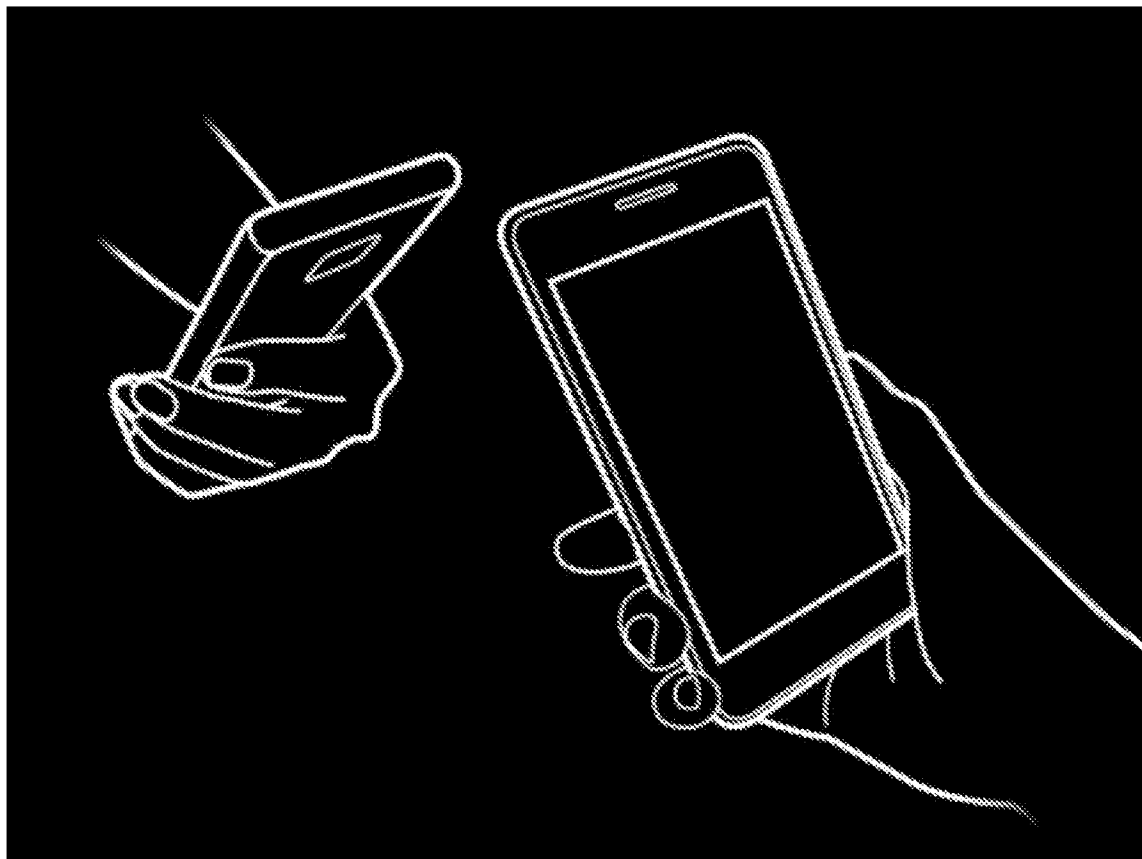
If you want to send large image, video or song files from one Galaxy S3 to another, Samsung has come up with S Beam. Here's how to use it.

---



**John Thompson** June 21, 2012 2:07 a.m. PT





over NFC to transmit information such as contact details and browser pages from one mobile to another. But it doesn't use Wi-Fi Direct so it's impractical for larger files.

By combining NFC and Wi-Fi Direct, S Beam is capable of sending larger files between phones, such as images, videos and music tracks. The transfer is initiated by NFC and the actual file transfer is handled using Wi-Fi Direct. This means you can expect transfer speeds of up to 300MBps.

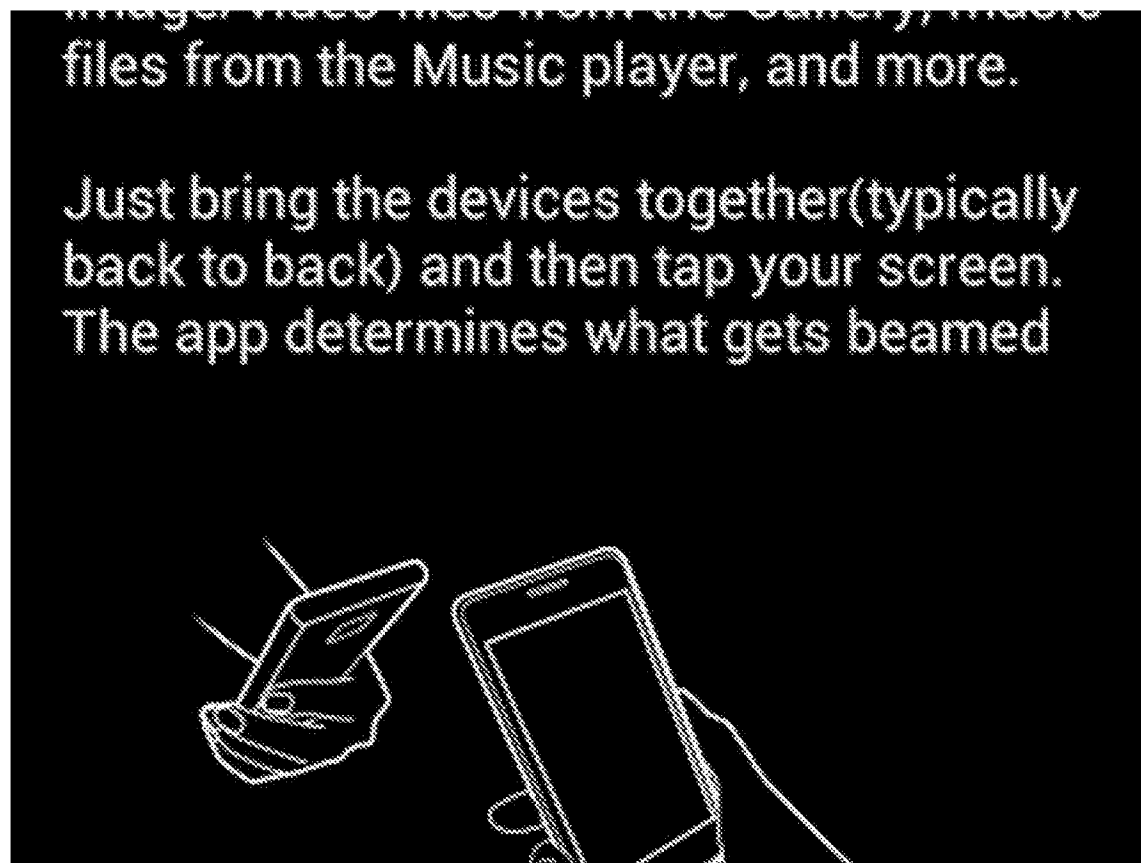
## How to enable S Beam

You can use videos, contacts, and more. Just bring the devices together (typically back to back) and then tap your screen. The app determines what is beamed

You can activate both Android Beam and S Beam through the Settings app on your Galaxy S3. To do this, go to Settings > More settings, and you will see separate entries for both. Tap on each of them to ensure that they are activated.

You will need to enable NFC in the same settings window as well, as this allows the phone to transfer information with other NFC-enabled devices.

## How to transfer files using S Beam



Transferring a file between two phones couldn't be simpler. You simply navigate to the image, video or music track that you want to send and hold the back of your phone against the back of another S Beam-capable device. Your phone will tell you to 'tap to beam', and the file transfer will begin.

As the transfer uses Wi-Fi Direct, you can then take the phones away from each other and the transfer will continue uninterrupted. You don't need to be connected to the same network for this -- it all happens automatically between the phones.

At the moment, S Beam is only available on the Galaxy S3, although as Samsung continues to release more Android 4.0 devices, you will be able to transfer files in this way between more models. You can use the Android Beam functionality with any phone running Android 4.0 or later that has NFC capabilities.



How To



How To





**MEDIA ALERT**

October 28, 2013

# Apple Reports Fourth Quarter Results

## iPhone Sales Grow 26% to Establish New September Quarter Record

CUPERTINO, California—October 28, 2013—Apple® today announced financial results for its fiscal 2013 fourth quarter ended September 28, 2013. The Company posted quarterly revenue of \$37.5 billion and quarterly net profit of \$7.5 billion, or \$8.26 per diluted share. These results compare to revenue of \$36 billion and net profit of \$8.2 billion, or \$8.67 per diluted share, in the year-ago quarter. Gross margin was 37 percent compared to 40 percent in the year-ago quarter. International sales accounted for 60 percent of the quarter's revenue.

The Company sold 33.8 million iPhones, a record for the September quarter, compared to 26.9 million in the year-ago quarter. Apple also sold 14.1 million iPads during the quarter, compared to 14 million in the year-ago quarter. The Company sold 4.6 million Macs, compared to 4.9 million in the year-ago quarter.

Apple's Board of Directors has declared a cash dividend of \$3.05 per share of the Company's common stock. The dividend is payable on November 14, 2013, to shareholders of record as of the close of business on November 11, 2013.

"We're pleased to report a strong finish to an amazing year with record fourth quarter revenue, including sales of almost 34 million iPhones," said Tim Cook, Apple's CEO. "We're excited to go into the holidays with our new iPhone 5c and iPhone 5s, iOS 7, the new iPad mini with Retina Display and the incredibly thin and light iPad Air, new MacBook Pros, the radical new Mac Pro, OS X Mavericks and the next generation iWork and iLife apps for OS X and iOS."

"We generated \$9.9 billion in cash flow from operations and returned an additional \$7.8 billion in cash to shareholders through dividends and share repurchases during the September quarter, bringing cumulative payments under our capital return program to \$36 billion," said Peter Oppenheimer, Apple's CFO.

Apple is providing the following guidance for its fiscal 2014 first quarter:

- revenue between \$55 billion and \$58 billion
- gross margin between 36.5 percent and 37.5 percent
- operating expenses between \$4.4 billion and \$4.5 billion
- other income/(expense) of \$200 million
- tax rate of 26.25 percent

Apple will provide live streaming of its Q4 2013 financial results conference call beginning at 2:00 p.m. PDT on October 28, 2013 at [www.apple.com/quicktime/qtv/earningsq413](http://www.apple.com/quicktime/qtv/earningsq413). This webcast will also be available for replay for approximately two weeks thereafter.

This press release contains forward-looking statements including without limitation those about the Company's estimated revenue, gross margin, operating expenses, other income/(expense), and tax rate. These statements involve risks and uncertainties, and actual results may differ. Risks and uncertainties include without limitation the effect of competitive and economic factors, and the Company's reaction to those factors, on consumer and business buying decisions with respect to the Company's products; continued competitive pressures in the marketplace; the ability of the Company to deliver to the marketplace and stimulate customer demand for new programs, products, and technological innovations on a timely basis; the effect that product introductions and transitions, changes in product pricing or mix, and/or increases in component costs could have on the Company's gross margin; the inventory risk associated with the Company's need to order or commit to order product components in advance of customer orders; the continued availability on acceptable terms, or at all, of certain components and services essential to the Company's business currently obtained by the Company from sole or limited sources; the effect that the Company's dependency on manufacturing and logistics services provided by third parties may have on the quality, quantity or cost of products manufactured or services rendered; risks associated with the Company's international operations; the Company's reliance on third-party intellectual property and digital content; the potential impact of a finding that the Company has infringed on the intellectual property rights of others; the Company's dependency on the performance of distributors, carriers and other resellers of the Company's products; the effect that product and service quality problems could have on the Company's sales and operating profits; the continued service and availability of key executives and employees; war, terrorism, public health issues, natural

disasters, and other circumstances that could disrupt supply, delivery, or demand of products; and unfavorable results of other legal proceedings. More information on potential factors that could affect the Company's financial results is included from time to time in the "Risk Factors" and "Management's Discussion and Analysis of Financial Condition and Results of Operations" sections of the Company's public reports filed with the SEC, including the Company's Form 10-K for the fiscal year ended September 29, 2012, its Form 10-Q for the quarter ended December 29, 2012, its Form 10-Q for the quarter ended March 30, 2013, its Form 10-Q for the quarter ended June 29, 2013, and its Form 10-K for the year ended September 28, 2013 to be filed with the SEC. The Company assumes no obligation to update any forward-looking statements or information, which speak as of their respective dates.

Apple designs Macs, the best personal computers in the world, along with OS X, iLife, iWork and professional software. Apple leads the digital music revolution with its iPods and iTunes online store. Apple has reinvented the mobile phone with its revolutionary iPhone and App Store, and is defining the future of mobile media and computing devices with iPad.


**Press Contact:**

Steve Dowling  
Apple  
dowling@apple.com  
(408) 974-1896

**Investor Relations Contacts:**

Nancy Paxton  
Apple  
paxton1@apple.com  
(408) 974-5420

Joan Hoover  
Apple  
hoover1@apple.com  
(408) 974-4570

 **Data Summary**  
[View PDF](#)

# Newsroom

The latest news and updates, direct from Apple.

[Read more >](#)

Newsroom > [Apple Reports Fourth Quarter Results](#)

## Shop and Learn

- [Mac](#)
- [iPad](#)
- [iPhone](#)
- [Watch](#)
- [TV](#)
- [Music](#)
- [AirPods](#)
- [HomePod](#)
- [iPod touch](#)
- [Accessories](#)
- [Gift Cards](#)

## Services

- [Apple Music](#)
- [Apple TV+](#)
- [Apple Fitness+](#)
- [Apple News+](#)
- [Apple Arcade](#)
- [iCloud](#)
- [Apple One](#)
- [Apple Card](#)
- [Apple Books](#)
- [App Store](#)

## Account

- [Manage Your Apple ID](#)
- [Apple Store Account](#)
- [iCloud.com](#)

## Apple Store

- [Find a Store](#)
- [Shop Online](#)
- [Genius Bar](#)
- [Today at Apple](#)
- [Apple Camp](#)
- [Apple Store App](#)
- [Refurbished and Clearance](#)
- [Financing](#)
- [Apple Trade In](#)
- [Order Status](#)
- [Shopping Help](#)

## For Business

- [Apple and Business](#)
- [Shop for Business](#)

## For Education

- [Apple and Education](#)
- [Shop for K-12](#)
- [Shop for College](#)

## For Healthcare

- [Apple in Healthcare](#)
- [Health on Apple Watch](#)
- [Health Records on iPhone](#)

## For Government

- [Shop for Government](#)
- [Shop for Veterans and Military](#)

## Apple Values

- [Accessibility](#)
- [Education](#)
- [Environment](#)
- [Inclusion and Diversity](#)
- [Privacy](#)
- [Racial Equity and Justice](#)
- [Supplier Responsibility](#)

## About Apple

- [Newsroom](#)
- [Apple Leadership](#)
- [Job Opportunities](#)
- [Investors](#)
- [Events](#)
- [Contact Apple](#)

More ways to shop: Find an [Apple Store](#) or other retailer near you. Or call 1-800-MY-APPLE.

Copyright © 2021 Apple Inc. All rights reserved.

[Privacy Policy](#)

[Terms of Use](#)

[Sales and Refunds](#)

[Legal](#)

[Site Map](#)

[United States](#)



Espacenet

**Bibliographic data: CN204375056 (U) — 2015-06-03**

---

Vending machine with Baidu Wallet payment function

**Inventor(s):** XU HAIDONG; ZHAO XISHAN; WANG JISHENG; WU YUNGANG; ZHANG HONG; LU SHILONG; SUN YEPING; LI YOUHAO; YU LULU; DUAN HONGYAN; FU LIANHUA; HAN DONGLING ± (XU HAIDONG, ; ZHAO XISHAN, ; WANG JISHENG, ; WU YUNGANG, ; ZHANG HONG, ; LU SHILONG, ; SUN YEPING, ; LI YOUHAO, ; YU LULU, ; DUAN HONGYAN, ; FU LIANHUA, ; HAN DONGLING)

**Applicant(s):** QINGDAO EASY TOUCH DIGITAL TECHNOLOGY CO LTD ± (QINGDAO EASY TOUCH DIGITAL TECHNOLOGY CO., LTD)

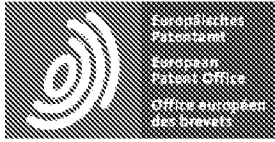
**Classification:** - **international:** G06Q20/12; G06Q20/32; G07F11/00  
- **cooperative:**

**Application number:** CN20152079858U 20150205

**Priority number(s):** CN20152079858U 20150205

**Abstract of CN204375056 (U)**

A vending machine with a Baidu Wallet payment function comprises a door body, a paper money device, a one-card card reader, a coin device, a touch control all-in-one machine, an induction card reader, a main control panel, a wireless router and a display window. The paper money device, the one-card card reader and the coin device are arranged on the left portion of the door body. The paper money device, the one-card card reader and the coin device are all connected with the main control panel. The induction card reader and the touch control all-in-one machine are arranged above the main control panel. The touch control all-in-one machine is connected with the main control panel. The touch control all-in-one machine comprises a touch screen, a display screen and an industrial personal computer, wherein the display screen and the industrial personnel computer are arranged above the touch screen. The wireless router and the display window are arranged on the right portion of the door body. The wireless router is connected with the touch control all-in-one machine through a cable. The vending machine is convenient to install, easy to use and operate, novel, powerful in function, rapid, easy and convenient to use, safe, reliable and worthy of vigorous popularization, and the vending machine has the Baidu Wallet payment function.



# Patent Translate

Powered by EPO and Google

## Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

## DESCRIPTION CN204375056U

*10* A vending machine with Paypay payment function

[0001]

*14* Technical field

[0002]

*18* The utility model relates to the field of automatic vending machines, in particular to an automatic vending machine with a Baifu payment function.

[0003]

*23* Background technique

[0004]

*27* There are generally two types of vending machines on the market based on payment methods: cash purchases and card purchases.

*29* The first method is the most traditional method, and the second method has begun to transition to cashless sales, but it is limited to small payments, and the proximity cards in various industries and regions are not unified. There are many consumer cards, which can no longer satisfy people. Growing consumer demand.

*32* With the increasing popularity of smartphones, the gradual rise of online shopping has given rise to an emerging consumption model - mobile shopping.

*34* Mobile shopping is shopping through mobile terminals and mobile networks, that is, a business model in which users use their mobile phones to pay for the goods or services they consume. Currently, banks, mobile operators, and third-party online payment companies all have different service models to meet the needs of different users. In recent years, mobile shopping has developed rapidly in the Chinese market. If this

Petitioner Exhibit 1002-4028

convenient touch shopping terminal with mobile phone payment function is embedded in a vending machine, not only can the traditional functions of the vending machine be retained, the advertising media function can be enriched and developed, but also the payment function of the vending machine can be improved. The function has achieved a qualitative leap.

[0005]

45 Utility model content

[0006]

49 The utility model aims to provide a vending machine that is easy to install, simple to use and operate, and has a BaiFuba payment function. The product is novel, powerful, quick and easy to use, safe and reliable, and has a BaiFuba payment function. .

[0007]

55 In order to achieve the above purpose, the present utility model provides the following technical solution: a vending machine with Baifu payment function, including a door body, a banknote dispenser, a card reader, a coin dispenser, a touch-control integrated machine, and an induction card reader. , main control board, wireless router and display window, the banknote device, card reader and coin device are located on the left side of the door, and the banknote device, card reader and coin device are all connected to the main control board; An induction card reader and a touch-control all-in-one machine are provided above the main control board, in which the touch-control all-in-one machine is connected to the main control board; the touch-control all-in-one machine includes a touch screen, a display screen and an industrial computer, wherein the display screen and the industrial computer are equipped with Above the touch screen; the wireless router and the display window are located on the right side of the door, and the wireless router is connected to the touch all-in-one machine through a network cable.

[0008]

69 As a further solution of the present invention: the one-card card reader is connected to the main control board through the vending machine MDB interface or serial port.

[0009]

74 As a further solution of the present invention: the induction card reader is connected to the main control board through a serial port.

[0010]

79 As a further solution of the present invention: the touch-integrated machine is connected to the main control

Petitioner Exhibit 1002-4029

board through an RS232 communication line.

[0011]

84 As a further solution of the present invention: a vending machine with a BaiFuba payment function is connected to a merchant server.

[0012]

89 Compared with the existing technology, the beneficial effects of the present utility model are: the vending machine with BaiFuba payment function can effectively and flexibly manage sales data and sales amounts, solving many management shortcomings of cash shopping in the past; mobile phone Installed with the Baidu client, the mobile Baidu shopping terminal only includes a touch-control all-in-one machine. Consumers can scan codes to pay for shopping through the mobile Baidu terminal. The mobile Baidu shopping terminal can be embedded in a vending machine, and The main control system of the vending machine is connected with the software to realize the shopping function of Baidu Pay on the mobile phone.

96 Baidu Wallet is associated with the consumer's Baidu Pay account. When the consumer pays, the mobile Baidu Pay scans the QR code to realize the docking payment between the consumer's mobile phone and the Baidu Pay shopping terminal. The merchant server is set up by the operator, to receive payment information and process refunds.

100 This product is universal among consumer groups, because mobile phones have become a must-have item for the public, and the use of Baidu clients is also increasing across the country. This payment method is very conducive to promotion, very convenient for consumers, and good for operators. It solves many management shortcomings of cash shopping.

104 This product is easy to install, simple to use and operate, and has BaiFu payment function. It is novel, powerful, quick and easy to use, safe and reliable, and deserves to be vigorously promoted.

[0013]

109 Description of the drawings

[0014]

113 Figure 1 is an overall schematic diagram of the utility model;

[0015]

117 Figure 2 is an overall schematic diagram of the merchant server.

[0016]

121 Detailed ways



[0017]

125 The technical solutions in the embodiments of the present utility model will be clearly and completely described below with reference to the accompanying drawings in the embodiments of the present utility model. Obviously, the described embodiments are only part of the embodiments of the present utility model, not all implementations. example.

129 Based on the embodiments of the present utility model, all other embodiments obtained by those of ordinary skill in the art without creative efforts fall within the scope of protection of the present utility model.

[0018]

134 Please refer to Figures 1-2. In the embodiment of the present invention, a vending machine with a BaiFuba payment function includes a door 1, a banknote dispenser 2, a card reader 3, a coin dispenser 4, and a touch-control integrated machine 5. Inductive card reader 6, main control board 7, wireless router 8 and display window 12. The banknote machine 2, card reader 3 and coin machine 4 are located on the left side of the door 1. The card reader 3 and the coin machine 4 are both connected to the main control board 7. The card reader 3 communicates with the main control board 7 through the vending machine M DB interface or serial port; an induction card reader is provided above the main control board 7. 6 and touch all-in-one machine 5, in which the induction card reader 6 is used to read UnionPay cards, the induction card reader 6 is connected to the main control board 7 through the serial port, and the touch all-in-one machine 5 is connected to the main control board 7 through the RS232 communication line, the software provided in the touch-control all-in-one machine 5 has the BaiFubao payment method, and consumers can scan the code to pay for shopping on the vending machine through BaiFubao on their mobile phones; the touch-control all-in-one machine 5 includes a touch screen 9, a display screen 10 and industrial computer 11, in which the display screen 10 and the industrial computer 11 are located above the touch screen 9; the wireless router 8 and the display window 12 are located on the right side of the door 1, and the wireless router 8 is connected to the touch all-in-one machine 5 through a network cable. Connection: The vending machine with Baifu payment function is connected to the merchant server 13. The merchant server 13 is set up by the operator to receive payment information, issue payment results to the vending machine and process refunds.

[0019]

155 When shopping, select the product you want to buy through the product selection buttons on the display window 12. At this time, you can not only choose traditional coin shopping, one-card shopping, UnionPay proximity card, but also mobile phone shopping.

158 After selecting the product to be purchased on the display window 12, select "Baidu Pay" as the shopping method of the sales software in the touch all-in-one machine 5. At this time, the sales software will splice a URL according to the rules of the document. Access to this URL will be based on the splicing time. Depending on the request parameters, a short URL or a QR code image corresponding to the short URL is returned. If a short URL is returned, the sales software will generate a QR code. At the same time, the sales software will open a long link to communicate with the merchant server and send a query whether the order

Petitioner Exhibit 1002-4031

payment was successful. Request, wait for scanning and payment, the user only needs to open the Baidu client on the smartphone, enter "My Wallet", click "Scan", align the scanned box with the QR code, and the client will display. After confirming the name and price of the product to be purchased, make the payment through the mobile Baidu payment platform. After the payment is successful, the Baidu payment platform will send the payment result to the merchant server. This notification can be sent within a few seconds after the payment is completed, ensuring real-time and retry after failure to ensure that the data can reach the operator's server. Then the merchant server responds to the payment success request sent by the sales software. The sales software transmits the transaction success information to the vending machine main control system. The vending machine main control system It will control the shipping organization to sell the goods purchased by the customer, and the front-end will ship the goods and send the successful shipment information to the merchant server, so that the merchant server will modify the order status.

175 When encountering overtime payment or shipment failure, the sales software will send a refund request to the server. The server can submit the refund request to the Baidu payment platform, and the Baidu payment platform will verify the signature. After the signature verification is passed, the refund will be executed. After the payment is successful, the Baidu payment platform will notify the merchant server of the payment result, so that the merchant server can promptly modify the refund status of the order.

[0020]

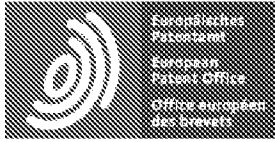
183 It is obvious to those skilled in the art that the present invention is not limited to the details of the above exemplary embodiments, and the present invention can be implemented in other specific forms without departing from the spirit or basic characteristics of the present invention.

186 Therefore, from any point of view, the embodiments should be regarded as exemplary and non-restrictive. The scope of the present invention is defined by the appended claims rather than the above description, and it is therefore intended that all claims falling within the rights All changes within the meaning and scope of the required equivalent elements are included in the present invention.

190 Any reference signs in the claims shall not be construed as limiting the claim in question.

[0021]

194 In addition, it should be understood that although this specification is described in terms of implementations, not each implementation only contains an independent technical solution. This description of the specification is only for the sake of clarity, and those skilled in the art should take the specification as a whole. , the technical solutions in each embodiment can also be appropriately combined to form other implementations that can be understood by those skilled in the art.



# Patent Translate

Powered by EPO and Google

## Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

## CLAIMS CN204375056U

1.

13 A vending machine with a Baidu payment function, including a door (1), a banknote machine (2), a card reader (3), a coin machine (4), a touch-control integrated machine (5), and an induction reader Card device (6), main control board (7), wireless router (8) and display window (12), characterized in that the banknote device (2), all-in-one card reader (3) and coin device (4) Located on the left side of the door (1), the banknote machine (2), card reader (3) and coin machine (4) are all connected to the main control board (7); above the main control board (7) It is provided with an induction card reader (6) and a touch all-in-one machine (5), wherein the touch all-in-one machine (5) is connected to the main control board (7); the touch all-in-one machine (5) includes a touch screen (9), Display screen (10) and industrial computer (11), wherein the display screen (10) and industrial computer (11) are located above the touch screen (9); the wireless router (8) and display window (12) are located on the door (1) On the right side, the wireless router (8) is connected to the touch all-in-one machine (5) through a network cable.

2.

27 A vending machine with BaiFuba payment function according to claim 1, characterized in that the one-card reader (3) is connected to the main control board (7) through the vending machine M DB interface or serial port.

3.

33 A vending machine with BaiFuba payment function according to claim 1, characterized in that the induction card reader (6) is connected to the main control board (7) through a serial port.

4.

38 A vending machine with a BaiFuba payment function according to claim 1, characterized in that the touch-integrated machine (5) is connected to the main control board (7) through an RS232 communication line.

5.

43 An automatic vending machine with BaiFubao payment function according to claim 1, characterized in that the vending machine with BaiFubao payment function is connected to the merchant server (13).



(12) 实用新型专利

(10) 授权公告号 CN 204375056 U

(45) 授权公告日 2015.06.03

(21) 申请号 201520079858.1

(22) 申请日 2015.02.05

(73) 专利权人 青岛易触数码科技有限公司

地址 266555 山东省青岛市黄岛区松花江路  
82号

(72) 发明人 徐海东 赵希善 王积升 武云刚  
张红 卢世龙 孙业平 李友好  
于露露 段红岩 付连华 韩冬玲

(51) Int. Cl.

G07F 11/00(2006.01)

G06Q 20/32(2012.01)

G06Q 20/12(2012.01)

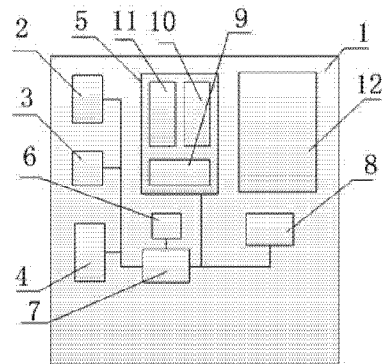
权利要求书1页 说明书3页 附图1页

(54) 实用新型名称

一种具有百付宝支付功能的自动售货机

(57) 摘要

一种具有百付宝支付功能的自动售货机,包括门体、纸币器、一卡通读卡器、硬币器、触控一体机、感应读卡器、主控板、无线路由器和展示窗,所述纸币器、一卡通读卡器和硬币器设于门体左部,该纸币器、一卡通读卡器和硬币器均与主控板连接;所述主控板的上方设有感应读卡器和触控一体机,其中触控一体机与主控板连接;所述触控一体机包括触摸屏、显示屏和工控机,其中显示屏和工控机设于触摸屏的上方;所述无线路由器和展示窗设于门体右部,其中无线路由器通过网线与触控一体机连接;本产品安装方便,使用、操作简单,具有百付宝支付功能,产品新颖,功能强大,使用快捷简便,安全可靠,值得大力推广。



CN 204375056 U

1. 一种具有百付宝支付功能的自动售货机,包括门体(1)、纸币器(2)、一卡通读卡器(3)、硬币器(4)、触控一体机(5)、感应读卡器(6)、主控板(7)、无线路由器(8)和展示窗(12),其特征在于,所述纸币器(2)、一卡通读卡器(3)和硬币器(4)设于门体(1)左部,该纸币器(2)、一卡通读卡器(3)和硬币器(4)均与主控板(7)连接;所述主控板(7)的上方设有感应读卡器(6)和触控一体机(5),其中触控一体机(5)与主控板(7)连接;所述触控一体机(5)包括触摸屏(9)、显示屏(10)和工控机(11),其中显示屏(10)和工控机(11)设于触摸屏(9)的上方;所述无线路由器(8)和展示窗(12)设于门体(1)右部,其中无线路由器(8)通过网线与触控一体机(5)连接。

2. 根据权利要求1所述的一种具有百付宝支付功能的自动售货机,其特征在于,所述一卡通读卡器(3)通过售货机MDB接口或串口与主控板(7)连接。

3. 根据权利要求1所述的一种具有百付宝支付功能的自动售货机,其特征在于,所述感应读卡器(6)通过串口与主控板(7)连接。

4. 根据权利要求1所述的一种具有百付宝支付功能的自动售货机,其特征在于,所述触控一体机(5)通过RS232通讯线与主控板(7)连接。

5. 根据权利要求1所述的一种具有百付宝支付功能的自动售货机,其特征在于,一种具有百付宝支付功能的自动售货机与商户服务器(13)连接。

## 一种具有百付宝支付功能的自动售货机

### 技术领域

[0001] 本实用新型涉及自动售货机领域,尤其是一种具有百付宝支付功能的自动售货机。

### 背景技术

[0002] 市面上自动售货机按照支付方式分类大体有两种:现金购物和刷卡购物。第一种方式是最传统的方式,第二种方式已经开始向无钞售卖过渡,但是仅限于小额支付,并且各个行业、各个地区的感应卡不统一,消费者卡片繁多,已经不能满足人们日益增长的消费需求。随着智能手机的使用日益普及,网络购物的逐渐兴起,催生了一种新兴的消费模式——手机购物。手机购物就是通过移动终端手机网络进行购物,即用户用其手机对所消费的商品或服务进行账务支付的一种商业模式。目前银行、移动运营商、第三方在线支付公司都有各自不同的服务模式,来满足不同用户的使用需求。近年来,手机购物在中国市场发展迅速。如果在自动售货机中嵌入这种便捷的具有支持手机支付功能的触控购物终端,不仅能使自动售货机的传统功能保留,广告媒体功能得到丰富和发展,而且还能使自动售货机的支付功能得到质的飞跃。

### 实用新型内容

[0003] 本实用新型旨在提供一种安装方便,使用、操作简单,具有百付宝支付功能的自动售货机,产品新颖,功能强大,使用快捷简便,安全可靠的具有百付宝支付功能的自动售货机。

[0004] 为实现上述目的,本实用新型提供如下技术方案:一种具有百付宝支付功能的自动售货机,包括门体、纸币器、一卡通读卡器、硬币器、触控一体机、感应读卡器、主控板、无线路由器和展示窗,所述纸币器、一卡通读卡器和硬币器设于门体左部,该纸币器、一卡通读卡器和硬币器均与主控板连接;所述主控板的上方设有感应读卡器和触控一体机,其中触控一体机与主控板连接;所述触控一体机包括触摸屏、显示屏和工控机,其中显示屏和工控机设于触摸屏的上方;所述无线路由器和展示窗设于门体右部,其中无线路由器通过网线与触控一体机连接。

[0005] 作为本实用新型的进一步方案:所述一卡通读卡器通过售货机 MDB 接口或串口与主控板连接。

[0006] 作为本实用新型的进一步方案:所述感应读卡器通过串口与主控板连接。

[0007] 作为本实用新型的进一步方案:所述触控一体机通过 RS232 通讯线与主控板连接。

[0008] 作为本实用新型的进一步方案:一种具有百付宝支付功能的自动售货机与商户服务器连接。

[0009] 与现有技术相比,本实用新型的有益效果是:该具有百付宝支付功能的自动售货机,可以有效灵活的管理销售数据及销售金额,解决了以前现金购物存在的诸多管理弊端;

手机安装有百度客户端,手机百付宝购物终端仅仅包括触控一体机,消费者可以通过手机百付宝终端进行扫码支付购物,该手机百付宝购物终端可以嵌入到自动售货机上,与自动售货机的主控系统进行软件对接,实现手机百付宝购物功能。百度钱包关联消费者的百付宝账户,当消费者支付时,手机百付宝以扫描二维码的方式,实现消费者手机与百付宝购物终端的对接支付,商户服务器由运营商架设,来接收支付信息及处理退款。本产品具有消费群体的普遍性,因为手机已经成为大众必备用品,而且百度客户端的使用在全国范围内也在日渐增多,该支付方式非常利于推广,对消费者来说非常便捷,对运营商来说,解决了现金购物存在的诸多管理弊端。本产品安装方便,使用、操作简单,具有百付宝支付功能,产品新颖,功能强大,使用快捷简便,安全可靠,值得大力推广。

### 附图说明

[0010] 图 1 为本实用新型的整体示意图;

[0011] 图 2 为商户服务器的整体示意图。

### 具体实施方式

[0012] 下面将结合本实用新型实施例中的附图,对本实用新型实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本实用新型一部分实施例,而不是全部的实施例。基于本实用新型中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本实用新型保护的范围。

[0013] 请参阅图 1-2,本实用新型实施例中,一种具有百付宝支付功能的自动售货机,包括门体 1、纸币器 2、一卡通读卡器 3、硬币器 4、触控一体机 5、感应读卡器 6、主控板 7、无线路由器 8 和展示窗 12,所述纸币器 2、一卡通读卡器 3 和硬币器 4 设于门体 1 左部,该纸币器 2、一卡通读卡器 3 和硬币器 4 均与主控板 7 连接,一卡通读卡器 3 通过售货机 MDB 接口或串口与主控板 7 连接通讯;所述主控板 7 的上方设有感应读卡器 6 和触控一体机 5,其中感应读卡器 6 用于读取银联卡,感应读卡器 6 通过串口与主控板 7 连接,触控一体机 5 通过 RS232 通讯线与主控板 7 连接,触控一体机 5 内设定的软件具有百付宝支付方式,消费者可通过手机百付宝在自动售货机上进行扫码支付购物;所述触控一体机 5 包括触摸屏 9、显示屏 10 和工控机 11,其中显示屏 10 和工控机 11 设于触摸屏 9 的上方;所述无线路由器 8 和展示窗 12 设于门体 1 右部,其中无线路由器 8 通过网线与触控一体机 5 连接;该一种具有百付宝支付功能的自动售货机与商户服务器 13 连接,商户服务器 13 由运营商架设,来接收支付信息、给售货机下发支付结果及处理退款。

[0014] 在购物时通过展示窗 12 的选货按键选择想要购买的商品,此时不但可以选择传统的钱币购物,一卡通购物,银联感应卡,还可以选择手机购物。在展示窗 12 上面选择需要购买的商品之后,触控一体机 5 中售卖软件的购物方式选择“百度支付”,此时售卖软件将按照文档的规则拼接一个 URL,访问这个 URL 将根据其拼接时请求参数的不同返回短 URL 或短 URL 对应的二维码图片,如果返回短 URL,再由售卖软件生成二维码,同时售卖软件打开一个长链接和商户服务器通信,发送订单是否付款成功的查询请求,等待扫描并支付,用户只要打开智能手机上的百度客户端,进入“我的钱包”,点击“扫一扫”,将扫一扫的方框对准二维码,客户端上将显示要购买的商品的名称及价格,确认后通过手机百度支付平台进行



付款,支付成功后,百度支付平台将发送支付结果到商户服务器上,这个通知可在支付完成后几秒钟内发送,保证实时性,并在失败后重试,保证数据能到达运营商的服务器,然后商户服务器应答售卖软件发出的付款成功请求,售卖软件将交易成功信息传给自动售货机主控系统,售货机主控系统就会控制出货机构售出顾客所选购的商品,前端出货并发送出货成功的信息到商户服务器,这样商户服务器将此订单状态进行修改。遇到超时付款或出货失败的情况时,售卖软件将向服务器发送退款请求,服务器可以提交退款请求到百度支付平台,由百度支付平台进行验签,验签通过后执行退款,退款成功后,百度支付平台会通知商户服务器支付结果,这样,商户服务器就可以及时修改订单的退款状态。

[0015] 对于本领域技术人员而言,显然本实用新型不限于上述示范性实施例的细节,而且在不背离本实用新型的精神或基本特征的情况下,能够以其他的具体形式实现本实用新型。因此,无论从哪一点来看,均应将实施例看作是示范性的,而且是非限制性的,本实用新型的范围由所附权利要求而不是上述说明限定,因此旨在将落在权利要求的等同要件的含义和范围内的所有变化囊括在本实用新型内。不应将权利要求中的任何附图标记视为限制所涉及的权利要求。

[0016] 此外,应当理解,虽然本说明书按照实施方式加以描述,但并非每个实施方式仅包含一个独立的技术方案,说明书的这种叙述方式仅仅是为清楚起见,本领域技术人员应当将说明书作为一个整体,各实施例中的技术方案也可以经适当组合,形成本领域技术人员可以理解的其他实施方式。

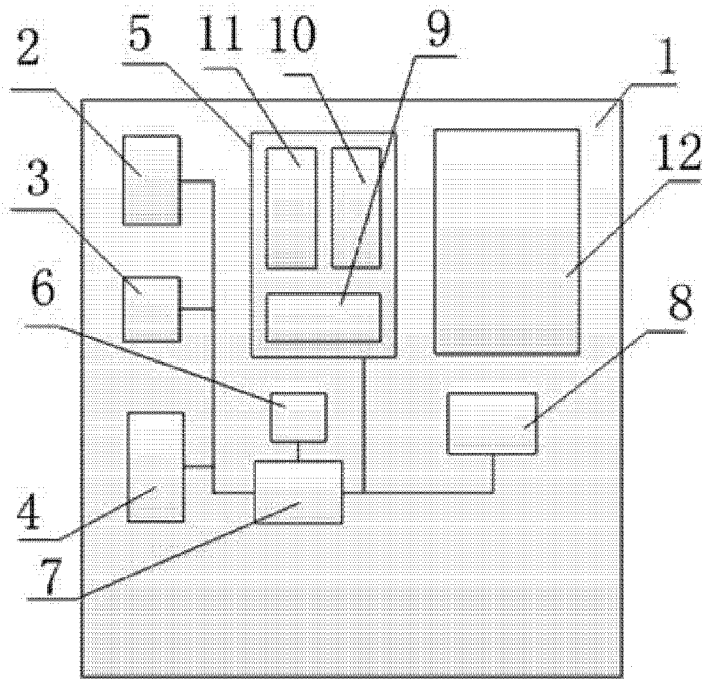


图 1

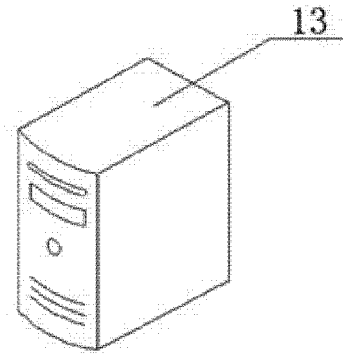
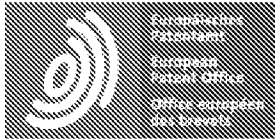


图 2



## Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

### DESCRIPTION CN107480975A

10 Drone sales method

[0001]

14 Technical field

[0002]

18 The present invention relates to the field of unmanned vending, and in particular to an unmanned aerial vehicle vending method.

[0003]

23 Background technique

[0004]

27 Existing vending drones (also known as: unmanned vending machines, abbreviated as: drones) are commonly used in shopping malls, parks, scenic spots and amusement places, etc., and can save human resources.

[0005]

32 However, vending drones often need to be illuminated continuously, especially when no one is around for a long time. This causes a waste of energy, which is heartbreaking and is not conducive to building a green, energy-saving and sustainable new China that advances with the times., and the goods displayed in the vending drone have been exposed to the sun for a long time and are easily oxidized.

[0006]

39 Contents of the invention

[0007]

43 Based on this, it is necessary to provide a drone vending machine to improve the problem of energy waste caused by constant lighting in vending drones and the fact that the goods displayed in vending drones are easily oxidized after being exposed to the sun for a long time. cargo method.

[0008]

49 A drone vending method includes the following steps: determine whether a user approaches, and if so, display the goods; further determine whether the handheld terminal enters a pre-payment state, and if so, provide goods on the shelf according to the user's choice; further determine whether If the provided goods are taken out from the shelf, the deduction will be completed based on the selling price of the provided goods; it will be judged whether the user has moved away, and if so, the display of the goods will be stopped.

[0009]

57 The above-mentioned drone sales method only displays the goods when the user approaches and stops displaying the goods when the user moves away. This eliminates the need for constant lighting, which causes energy waste, and avoids the displayed goods being easily oxidized by the sun for a long time, which shortens the shelf life of the goods. It is longer, and the payment is only completed when the user takes out the provided goods from the shelf, which provides users with more freedom of choice and is especially suitable for supporting projects related to the Belt and Road construction.

[0010]

66 In one of the embodiments, the handheld terminal scans the code to enter the preparatory payment state.

[0011]

70 In one embodiment, the handheld terminal scans the QR code or barcode to enter the payment preparation state.

[0012]

75 In one of the embodiments, the proximity sensing handheld terminal enters the payment preparation state.

[0013]

79 In one of the embodiments, NFC or RFID proximity sensing handheld terminal is used to enter the

preparatory payment state.

[0014]

84 In one embodiment, the products are displayed in the product area.

[0015]

88 In one embodiment, thermal induction is used to select items from the item area.

[0016]

92 In one embodiment, infrared sensing is used to select goods from the goods area.

[0017]

96 In one embodiment, a temperature sensing method is used to select items from the item area.

[0018]

100 In one embodiment, gravity sensing is used to select items from the item area.

[0019]

104 The above drone vending method can also sense or read the handheld terminal, and select goods from the goods area through a variety of methods. It is easy and flexible to use. While protecting the rights of users, it can also protect the rights of drone cargo owners. rights and interests, to achieve a win-win balance for both parties, and is especially suitable for supporting projects related to the Belt and Road construction.

[0020]

111 Description of the drawings

[0021]

115 Figure 1 is a schematic diagram of an embodiment of the present invention.

[0022]

119 Detailed ways

[0023]

123 In order to make the above objects, features and advantages of the present invention more obvious and easy to understand, the specific embodiments of the present invention will be described in detail below with reference to the accompanying drawings.

126 In the following description, numerous specific details are set forth in order to provide a thorough understanding of the invention.

128 However, the present invention can be implemented in many other ways different from those described here. Those skilled in the art can make similar improvements without departing from the connotation of the present invention. Therefore, the present invention is not limited to the specific embodiments disclosed below.

[0024]

135 It should be noted that when an element is referred to as being "mounted" or "disposed on" another element, it can be directly on the other element or intervening elements may also be present.

137 When an element is said to be "connected" to another element, it can be directly connected to the other element or there may also be intervening elements present.

139 The terms "vertical", "horizontal", "left", "right" and similar expressions used herein are for illustrative purposes only and do not represent the only implementation manner.

[0025]

144 Unless otherwise defined, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the technical field to which the invention belongs.

146 The terminology used herein is for the purpose of describing specific embodiments only and is not intended to limit the invention.

148 As used herein, the term "and/or" includes any and all combinations of one or more of the associated listed items.

[0026]

153 As shown in Figure 1, one embodiment of the present invention is a drone vending method applied to an unmanned vending machine. The drone vending method includes the following steps: determine whether a user approaches, and if so Display the goods; further determine whether the handheld terminal enters the pre-payment state, and if so, provide the goods on the shelf according to the user's choice; further determine whether to take out the provided goods from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether If the user moves away, the display of goods will stop.

159 The above-mentioned drone sales method only displays the goods when the user approaches and stops displaying the goods when the user moves away. This eliminates the need for constant lighting, which causes energy waste, and avoids the displayed goods being easily oxidized by the sun for a long time, which shortens the shelf life of the goods. It is longer, and the payment is only completed when the user takes out the provided goods from the shelf, which provides users with more freedom of choice and is especially suitable

Petitioner Exhibit 1002-4044

for supporting projects related to the Belt and Road construction.

[0027]

168 For example, in the drone sales method, it is judged whether the user is approaching, and if so, the goods are displayed. Otherwise, no operation is performed, that is, there is no need to display the goods; for example, in the drone sales method, it is further judged whether the handheld terminal has entered the preparatory payment mode. status, if the goods are provided on the shelf according to the user's choice, otherwise no operation is performed, that is, there is no need to provide goods on the shelf; for example, in the drone sales method, it is further determined whether to take out the provided goods from the shelf, then Deduction is completed based on the selling price of the goods provided, otherwise no operation is performed, that is, there is no need to perform a deduction operation; for example, in the drone sales method, it is judged whether the user is away, and if so, the display of the goods is stopped, otherwise the current interface is maintained, such as displaying products or providing products on the shelf according to the user's selection.

[0028]

181 In one of the embodiments, the handheld terminal scans the code to enter the preparatory payment state.

182 For example, a drone vending method includes the following steps: determine whether the user is approaching, and if so, display the goods; further determine whether the handheld terminal enters the preparatory payment state by scanning the code, and if so, provide it on the shelf according to the user's choice goods; further determine whether to take out the provided goods from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether the user has moved away, and if so, stop displaying the goods.

188 For example, the user scans the QR code with his mobile phone to enter the payment preparation state.

189 In one embodiment, the handheld terminal scans the QR code or barcode to enter the payment preparation state.

191 In one of the embodiments, the proximity sensing handheld terminal enters the payment preparation state.

192 For example, a drone vending method includes the following steps: determine whether the user is approaching, and if so, display the goods; further determine whether the handheld terminal enters the payment preparation state through proximity sensing, and if so, display the goods on the shelf according to the user's choice Provide the goods; further determine whether to take out the provided goods from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether the user has moved away, and if so, stop displaying the goods.

198 For example, the user holds the mobile phone for proximity sensing and enters the ready payment state.

199 In one of the embodiments, NFC or RFID proximity sensing handheld terminal is used to enter the preparatory payment state.

201 In this way, you only need to hold the terminal to enter the preparatory payment state.

[0029]

205 One example is to associate the preparatory payment status with the user's identity information (such as ID, Petitioner Exhibit 1002-4045

number). Since the user's identity information is often unique, the corresponding user is also unique. In this way, the payment can be better ensured. payment situation.

208 For example, after determining that the handheld terminal enters the preparatory payment state, and before providing goods on the shelf according to the user's selection, the method further includes the following steps: associating the preparatory payment state with the user's identity information, and determining the user's payment based on the user's historical transaction records. If the credit meets a certain credit threshold, follow-up steps will be performed; that is, based on the user's historical transaction records, it is determined that the payment credit meets a certain credit threshold, and then the goods are provided on the shelf according to the user's choice, or it is determined to enter the prepayment state. , the provision of goods on the shelf according to the user's selection specifically includes the following steps: the preliminary payment status is associated with the user's identity information, and when it is determined that the user's payment credit meets a certain credit threshold based on the user's historical transaction records, according to the user's selection Provide goods on the shelves; among them, the credit threshold can be flexibly set based on experience, bank credit and/or social credit information.

220 For example, after determining the user's choice (that is, the user selects goods) and before providing the goods on the shelf, the method further includes the step of querying the user's payment ability according to the preliminary payment status, and when the payment ability meets the selected goods, the subsequent steps are performed. step, that is, providing goods on the shelves when the user's paying ability meets his or her choice.

225 In this way, users can avoid intentional overdraft consumption, and can also avoid users' non-subjective malicious overdraft consumption, especially face-saving consumption that cannot be controlled by people with incomplete behavioral capabilities, etc., which is conducive to safeguarding the interests of users, correctly guiding users to reasonable consumption, and thus effectively Maintained normal social order.

[0030]

232 In one embodiment, static pictures are used to display goods, for example, multiple static pictures are used to display multiple goods, or multiple static pictures are used to display one product, or one static picture is used to display one product.

235 In one embodiment, after displaying the goods and before providing the goods on the shelf according to the user's selection, the step further includes: clicking on the static picture to select the goods.

237 For example, before or after further determining whether the handheld terminal enters the ready-to-pay state, click on the static picture to select goods, and then when or after the hand-held terminal enters the ready-to-pay state, provide goods on the shelf according to the user's selection.

240 For example, a drone vending method includes the following steps: determine whether a user is approaching, and if so, use a static picture to display the goods; click on the static picture to select the goods; further determine whether the handheld terminal enters a ready payment state, and if so, use a static picture to display the goods; Choose to provide goods on the shelf; further determine whether to take out the provided goods from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether the user has moved away, and if so, stop displaying the goods.

246 In one embodiment, click on a static image to select a product corresponding to the static image.

247 In one embodiment, a number of static pictures are clicked during a preset time period, and a number of



products corresponding to the several static pictures are selected.

249 For example, a drone vending method includes the following steps: determine whether a user approaches, and if so, use a static image to display the product; click on a static image to select a product corresponding to the static image; further determine whether the handheld terminal has entered In the ready payment state, the goods are provided on the shelf according to the user's choice; it is further judged whether to take out the provided goods from the shelf, and if so, the deduction is completed based on the selling price of the provided goods; it is judged whether the user is away, and if so, the display of the goods is stopped. .

255 For example, a drone vending method includes the following steps: determine whether a user is approaching, and if so, use static pictures to display the goods; click on a number of static pictures during a preset time period, and select a number of goods corresponding to the static pictures. ; Further determine whether the handheld terminal enters the pre-payment state, and if so, provide goods on the shelf according to the user's choice; further determine whether the provided goods are taken out from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether the user has Stay away and the product will stop displaying.

262 In this way, multiple products can be given for users to choose at one time, thereby improving sales efficiency. After selection, if the provided goods are not taken out from the shelf, the drone can take back some or all of the provided goods, thus making Users can refuse to accept defective or unsatisfactory goods, avoiding the problem of being forced to accept defective or unsatisfactory goods.

[0031]

269 In one embodiment, dynamic images are used to display the goods.

270 In one embodiment, click on the dynamic image to select the item.

271 In one of the embodiments, several dynamic images are clicked within a preset time period, and several products corresponding to the several dynamic images are selected.

273 For example, a drone vending method includes the following steps: determine whether a user approaches, and if so, use static pictures and/or dynamic images to display the goods; click on a static picture to select a product corresponding to the static picture or click Choose a product through a dynamic image or click on a certain dynamic image to select a product corresponding to the dynamic image or click on several dynamic images during a preset time period to select several products corresponding to the several dynamic images; further determine whether the handheld terminal enters the preparatory payment state, yes Then provide the goods on the shelf according to the user's choice; further determine whether to take out the provided goods from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether the user has moved away, and if so, stop displaying the goods.

282 In this way, more complete and clearer information can be provided, and targeted advertising effects can be achieved to a certain extent.

[0032]

287 In one embodiment, the goods are displayed in the goods area. For example, it is determined whether the user approaches, and if so, the goods are displayed in the goods area.

289 For example, use a certain area of the unmanned vending machine as the product area and display the

products in the product area. For another example, the products are displayed on a display screen of an unmanned vending machine, such as a liquid crystal display screen. In other words, the goods can be displayed in real form, or only virtual pictures or text can be given to display the goods. For example, a drone vending method includes the following steps: determine whether the user is approaching, and if so, display the goods in the goods area; further determine whether the handheld terminal enters the payment preparation state, and if so, provide the goods on the shelf according to the user's choice goods; further determine whether to take out the provided goods from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether the user has moved away, and if so, stop displaying the goods. For example, the deduction is completed based on the selling price of one item taken out from the shelf, or the deduction is completed based on the total selling price of multiple items taken out from the shelf.

[0033]

303 For example, after the goods are displayed in the goods area and before it is further determined whether the handheld terminal enters the payment preparation state, a step is also included: selecting goods from the goods area.

306 For example, a drone vending method includes the following steps: determine whether the user is approaching, and if so, display the goods in the goods area; select the goods from the goods area; further determine whether the handheld terminal enters the ready payment state, and if so, according to the user Choose to provide the goods on the shelf; further determine whether to take out the provided goods from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether the user has moved away, and if so, stop displaying the goods. In one embodiment, thermal induction is used to select items from the item area. For example, users can select products from the product area by touching or approaching the product area with their fingers or palms. For example, a drone vending method includes the following steps: determine whether the user is approaching, and if so, display the goods in the goods area; use thermal induction to select goods from the goods area; further determine whether the handheld terminal enters the payment preparation state, If it is, the goods will be provided on the shelf according to the user's choice; if it is further judged whether to take out the provided goods from the shelf, if it is, the deduction will be completed based on the selling price of the provided goods; if it is judged whether the user has moved away, if so, the display of the goods will be stopped. In one embodiment, infrared sensing is used to select goods from the goods area. In one embodiment, a temperature sensing method is used to select items from the item area.

[0034]

325 In one embodiment, gravity sensing is used to select items from the item area.

326 For example, the user selects goods from the goods area by pressing or stepping. For example, a drone vending method includes the following steps: determine whether the user is approaching, and if so, display the goods in the goods area; use gravity sensing to select goods from the goods area; further determine whether the handheld terminal enters the payment preparation state, If it is, the goods will be provided on the shelf according to the user's choice; if it is further judged whether to take out the provided goods from the shelf, if it is, the deduction will be completed based on the selling price of the provided goods; if it is judged

whether the user has moved away, if so, the display of the goods will be stopped.

[0035]

336 The above drone vending method can also sense or read the handheld terminal, and select goods from the goods area through a variety of methods. It is easy and flexible to use. While protecting the rights of users, it can also protect the rights of drone cargo owners, rights and interests, to achieve a win-win balance for both parties, and is especially suitable for supporting projects related to the Belt and Road construction.

[0036]

343 One example is that the drone is provided with a waiting area and/or a sales area; for example, when in use, the user enters the sales area from the outside; for example, enters the sales area from the waiting area; another example is that the sales area is open, semi-open or closed setting; for example, determine whether the user approaches, specifically determine whether the user approaches the waiting area and/or sales area; for example, determine whether the user approaches the waiting area, and if so, display the goods; another example, Determine whether the user is close to the sales area, and if so, display the goods; for example, determine whether the handheld terminal enters the pre-payment state, and if so, allow the user to enter the sales area, and provide goods on the shelf according to the user's selection; for example, the goods area setting In the sales area; for example, after determining whether the handheld terminal enters the pre-payment state, and before providing goods on the shelf according to the user's selection, it also includes the steps of: sending a request to obtain the user's video permission; when the request to obtain the user's video permission is When passed, the user is allowed to enter the sales area; the video of the user in the sales area is obtained; after the user enters the sales area, goods are provided on the shelf according to the user's choice.

356 For example, a drone vending method includes the following steps: determine whether the user is approaching, and if so, display the goods; further determine whether the handheld terminal enters the payment preparation state, and if so, send a request to obtain the user's video permission; when obtaining the user When the video permission request is passed, the user is allowed to enter the sales area; the user's video in the sales area is obtained; goods are provided on the shelf according to the user's choice; further it is judged whether to take out the provided goods from the shelf, and if so, the goods are provided based on the user's choice. The sales price is deducted; it is determined whether the user is away, and if so, the display of the goods will be stopped.

364 For another example, completing the deduction based on the selling price of the provided goods specifically includes the following steps: when the user leaves the sales area, determine whether an abnormal operation occurs based on the video, otherwise, complete the deduction based on the selling price of the provided goods. In one embodiment, it is determined based on the video whether an abnormal operation occurs, and if so, an alarm signal is issued. For example, an alarm signal is sent to the monitoring room or management area to remind managers to handle it; another example is to send an alarm signal to the sales area to remind users to stop abnormal operations; another example is to send alarm information to managers or police officers. In one embodiment, the abnormal operation includes malicious damage or destruction behavior. In one of the embodiments, the method further includes the following steps: when the user is in the sales area, determine whether an abnormal operation occurs based on the video, and if so, send an alarm signal. In one

Petitioner Exhibit 1002-4049

embodiment, the method further includes the following steps: when the user is in the sales area, determine whether an abnormality occurs based on the video, and if so, send a help signal. For example, when the user is unwell, it can be handled in time, such as rescuing the user in time. In this way, it reflects better humanistic care and improves the safety factor of drones.

[0037]

381 In one embodiment, a body-worn video device is used to obtain videos of users in the sales area.  
382 For example, the user's mobile phone is used to wirelessly connect to the server to obtain the video of the user in the sales area. For another example, when the user is allowed to enter the sales area, the user is provided with a portable video device. The portable video device includes a wearable device and a number of cameras installed on the wearable device to obtain at least three views of the user in the sales area. Videos from various angles, including videos in front of the user, behind the user, and in front of the user including parts of the user. In one embodiment, a fixed video device installed in the sales area is used to obtain the user's video in the sales area. In one embodiment, when a user is allowed to enter the sales area, a positioning tag is set for the user; when a video of the user in the sales area is obtained, a video of the user in the sales area is obtained based on the positioning tag. For example, the positioning tag is a mobile phone that confirms the mobile phone identification code or its mobile phone identification code.

[0038]

395 In one embodiment, only one user is allowed into the vending area at a time.  
396 In this case, the user is required to come out of the sales area within a certain time. The following embodiments optimize this design. In one of the embodiments, after the user is allowed to enter the sales area, the following steps are also performed simultaneously: starting a timer; and prompting the user to leave the sales area after a certain period of time. In this way, the time when users enter the store can be controlled. In one of the embodiments, it is determined whether any user among several users enters the prepayment state, and if so, all users are allowed to enter the sales area. In this way, local tyrants can bring their friends into the sales area, and parents can bring their children into the sales area. One person pays the bill and everyone benefits. For another example, when or after all users enter the sales area, steps are also executed simultaneously: start timing; and prompt users to leave the sales area after a certain period of time. In one embodiment, after allowing the user to enter the sales area, the step further includes: starting a timer; and prompting the user to leave the sales area after a certain period of time. For example, the certain time period is 1 minute, 5 minutes or 10 minutes, depending on the quantity of drone goods, and the cargo owner can also customize the certain time period, thus facilitating the cargo owner's time management and control.

[0039]

412 An example is that after completing the deduction based on the selling price of the goods provided, it also includes the step of sending information about the goods that were deducted, for example, to a preset terminal or server, so that the owner of the goods can clearly know the sales status of the goods.  
415 Another example is sending information about deducted goods regularly; for example, sending it once an

hour, or once a day, and so on. For example, when sending information about deducted goods, the identity information of the drone where the goods are located is attached. For example, the identity information is the serial number or serial number of the drone; in this way, it is helpful for the cargo owner to manage multiple drones. .

[0040]

423 It should be noted that other embodiments of the present invention also include an implementable drone vending method formed by combining the technical features in the above embodiments.

[0041]

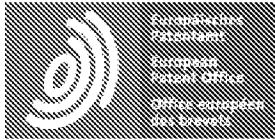
428 The technical features of the above-described embodiments can be combined in any way. To simplify the description, not all possible combinations of the technical features in the above-described embodiments are described. However, as long as there is no contradiction in the combination of these technical features, All should be considered to be within the scope of this manual.

[0042]

435 The above-mentioned embodiments only express several implementation modes of the present invention. The descriptions are relatively specific and detailed, but they should not be construed as limiting the scope of the invention.

438 It should be noted that, for those of ordinary skill in the art, several modifications and improvements can be made without departing from the concept of the present invention, and these all belong to the protection scope of the present invention.

441 Therefore, the scope of protection of the patent of the present invention should be determined by the appended claims.



## Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

### DESCRIPTION CN107480975A

10 Drone sales method

[0001]

14 Technical field

[0002]

18 The present invention relates to the field of unmanned vending, and in particular to an unmanned aerial vehicle vending method.

[0003]

23 Background technique

[0004]

27 Existing vending drones (also known as: unmanned vending machines, abbreviated as: drones) are commonly used in shopping malls, parks, scenic spots and amusement places, etc., and can save human resources.

[0005]

32 However, vending drones often need to be illuminated continuously, especially when no one is around for a long time. This causes a waste of energy, which is heartbreaking and is not conducive to building a green, energy-saving and sustainable new China that advances with the times., and the goods displayed in the vending drone have been exposed to the sun for a long time and are easily oxidized.

[0006]

39 Contents of the invention

[0007]

43 Based on this, it is necessary to provide a drone vending machine to improve the problem of energy waste caused by constant lighting in vending drones and the fact that the goods displayed in vending drones are easily oxidized after being exposed to the sun for a long time. cargo method.

[0008]

49 A drone vending method includes the following steps: determine whether a user approaches, and if so, display the goods; further determine whether the handheld terminal enters a pre-payment state, and if so, provide goods on the shelf according to the user's choice; further determine whether If the provided goods are taken out from the shelf, the deduction will be completed based on the selling price of the provided goods; it will be judged whether the user has moved away, and if so, the display of the goods will be stopped.

[0009]

57 The above-mentioned drone sales method only displays the goods when the user approaches and stops displaying the goods when the user moves away. This eliminates the need for constant lighting, which causes energy waste, and avoids the displayed goods being easily oxidized by the sun for a long time, which shortens the shelf life of the goods. It is longer, and the payment is only completed when the user takes out the provided goods from the shelf, which provides users with more freedom of choice and is especially suitable for supporting projects related to the Belt and Road construction.

[0010]

66 In one of the embodiments, the handheld terminal scans the code to enter the preparatory payment state.

[0011]

70 In one embodiment, the handheld terminal scans the QR code or barcode to enter the payment preparation state.

[0012]

75 In one of the embodiments, the proximity sensing handheld terminal enters the payment preparation state.

[0013]

79 In one of the embodiments, NFC or RFID proximity sensing handheld terminal is used to enter the

Petitioner Exhibit 1002-4053

preparatory payment state.

[0014]

84 In one embodiment, the products are displayed in the product area.

[0015]

88 In one embodiment, thermal induction is used to select items from the item area.

[0016]

92 In one embodiment, infrared sensing is used to select goods from the goods area.

[0017]

96 In one embodiment, a temperature sensing method is used to select items from the item area.

[0018]

100 In one embodiment, gravity sensing is used to select items from the item area.

[0019]

104 The above drone vending method can also sense or read the handheld terminal, and select goods from the goods area through a variety of methods. It is easy and flexible to use. While protecting the rights of users, it can also protect the rights of drone cargo owners. rights and interests, to achieve a win-win balance for both parties, and is especially suitable for supporting projects related to the Belt and Road construction.

[0020]

111 Description of the drawings

[0021]

115 Figure 1 is a schematic diagram of an embodiment of the present invention.

[0022]

119 Detailed ways



[0023]

123 In order to make the above objects, features and advantages of the present invention more obvious and easy to understand, the specific embodiments of the present invention will be described in detail below with reference to the accompanying drawings.

126 In the following description, numerous specific details are set forth in order to provide a thorough understanding of the invention.

128 However, the present invention can be implemented in many other ways different from those described here. Those skilled in the art can make similar improvements without departing from the connotation of the present invention. Therefore, the present invention is not limited to the specific embodiments disclosed below.

[0024]

135 It should be noted that when an element is referred to as being "mounted" or "disposed on" another element, it can be directly on the other element or intervening elements may also be present.

137 When an element is said to be "connected" to another element, it can be directly connected to the other element or there may also be intervening elements present.

139 The terms "vertical", "horizontal", "left", "right" and similar expressions used herein are for illustrative purposes only and do not represent the only implementation manner.

[0025]

144 Unless otherwise defined, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the technical field to which the invention belongs.

146 The terminology used herein is for the purpose of describing specific embodiments only and is not intended to limit the invention.

148 As used herein, the term "and/or" includes any and all combinations of one or more of the associated listed items.

[0026]

153 As shown in Figure 1, one embodiment of the present invention is a drone vending method applied to an unmanned vending machine. The drone vending method includes the following steps: determine whether a user approaches, and if so Display the goods; further determine whether the handheld terminal enters the pre-payment state, and if so, provide the goods on the shelf according to the user's choice; further determine whether to take out the provided goods from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether If the user moves away, the display of goods will stop.

159 The above-mentioned drone sales method only displays the goods when the user approaches and stops displaying the goods when the user moves away. This eliminates the need for constant lighting, which causes energy waste, and avoids the displayed goods being easily oxidized by the sun for a long time, which shortens the shelf life of the goods. It is longer, and the payment is only completed when the user takes out the provided goods from the shelf, which provides users with more freedom of choice and is especially suitable

for supporting projects related to the Belt and Road construction.

[0027]

168 For example, in the drone sales method, it is judged whether the user is approaching, and if so, the goods are displayed. Otherwise, no operation is performed, that is, there is no need to display the goods; for example, in the drone sales method, it is further judged whether the handheld terminal has entered the preparatory payment mode. status, if the goods are provided on the shelf according to the user's choice, otherwise no operation is performed, that is, there is no need to provide goods on the shelf; for example, in the drone sales method, it is further determined whether to take out the provided goods from the shelf, then Deduction is completed based on the selling price of the goods provided, otherwise no operation is performed, that is, there is no need to perform a deduction operation; for example, in the drone sales method, it is judged whether the user is away, and if so, the display of the goods is stopped, otherwise the current interface is maintained, such as displaying products or providing products on the shelf according to the user's selection.

[0028]

181 In one of the embodiments, the handheld terminal scans the code to enter the preparatory payment state.

182 For example, a drone vending method includes the following steps: determine whether the user is approaching, and if so, display the goods; further determine whether the handheld terminal enters the preparatory payment state by scanning the code, and if so, provide it on the shelf according to the user's choice goods; further determine whether to take out the provided goods from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether the user has moved away, and if so, stop displaying the goods.

188 For example, the user scans the QR code with his mobile phone to enter the payment preparation state.

189 In one embodiment, the handheld terminal scans the QR code or barcode to enter the payment preparation state.

191 In one of the embodiments, the proximity sensing handheld terminal enters the payment preparation state.

192 For example, a drone vending method includes the following steps: determine whether the user is approaching, and if so, display the goods; further determine whether the handheld terminal enters the payment preparation state through proximity sensing, and if so, display the goods on the shelf according to the user's choice Provide the goods; further determine whether to take out the provided goods from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether the user has moved away, and if so, stop displaying the goods.

198 For example, the user holds the mobile phone for proximity sensing and enters the ready payment state.

199 In one of the embodiments, NFC or RFID proximity sensing handheld terminal is used to enter the preparatory payment state.

201 In this way, you only need to hold the terminal to enter the preparatory payment state.

[0029]

205 One example is to associate the preparatory payment status with the user's identity information (such as ID

number). Since the user's identity information is often unique, the corresponding user is also unique. In this way, the payment can be better ensured. payment situation.

208 For example, after determining that the handheld terminal enters the preparatory payment state, and before providing goods on the shelf according to the user's selection, the method further includes the following steps: associating the preparatory payment state with the user's identity information, and determining the user's payment based on the user's historical transaction records. If the credit meets a certain credit threshold, follow-up steps will be performed; that is, based on the user's historical transaction records, it is determined that the payment credit meets a certain credit threshold, and then the goods are provided on the shelf according to the user's choice, or it is determined to enter the prepayment state. , the provision of goods on the shelf according to the user's selection specifically includes the following steps: the preliminary payment status is associated with the user's identity information, and when it is determined that the user's payment credit meets a certain credit threshold based on the user's historical transaction records, according to the user's selection Provide goods on the shelves; among them, the credit threshold can be flexibly set based on experience, bank credit and/or social credit information.

220 For example, after determining the user's choice (that is, the user selects goods) and before providing the goods on the shelf, the method further includes the step of querying the user's payment ability according to the preliminary payment status, and when the payment ability meets the selected goods, the subsequent steps are performed. step, that is, providing goods on the shelves when the user's paying ability meets his or her choice.

225 In this way, users can avoid intentional overdraft consumption, and can also avoid users' non-subjective malicious overdraft consumption, especially face-saving consumption that cannot be controlled by people with incomplete behavioral capabilities, etc., which is conducive to safeguarding the interests of users, correctly guiding users to reasonable consumption, and thus effectively Maintained normal social order.

[0030]

232 In one embodiment, static pictures are used to display goods, for example, multiple static pictures are used to display multiple goods, or multiple static pictures are used to display one product, or one static picture is used to display one product.

235 In one embodiment, after displaying the goods and before providing the goods on the shelf according to the user's selection, the step further includes: clicking on the static picture to select the goods.

237 For example, before or after further determining whether the handheld terminal enters the ready-to-pay state, click on the static picture to select goods, and then when or after the hand-held terminal enters the ready-to-pay state, provide goods on the shelf according to the user's selection.

240 For example, a drone vending method includes the following steps: determine whether a user is approaching, and if so, use a static picture to display the goods; click on the static picture to select the goods; further determine whether the handheld terminal enters a ready payment state, and if so, use a static picture to display the goods; Choose to provide goods on the shelf; further determine whether to take out the provided goods from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether the user has moved away, and if so, stop displaying the goods.

246 In one embodiment, click on a static image to select a product corresponding to the static image.

247 In one embodiment, a number of static pictures are clicked during a preset time period, and a number of

products corresponding to the several static pictures are selected.

249 For example, a drone vending method includes the following steps: determine whether a user approaches, and if so, use a static image to display the product; click on a static image to select a product corresponding to the static image; further determine whether the handheld terminal has entered In the ready payment state, the goods are provided on the shelf according to the user's choice; it is further judged whether to take out the provided goods from the shelf, and if so, the deduction is completed based on the selling price of the provided goods; it is judged whether the user is away, and if so, the display of the goods is stopped. .

255 For example, a drone vending method includes the following steps: determine whether a user is approaching, and if so, use static pictures to display the goods; click on a number of static pictures during a preset time period, and select a number of goods corresponding to the static pictures. ; Further determine whether the handheld terminal enters the pre-payment state, and if so, provide goods on the shelf according to the user's choice; further determine whether the provided goods are taken out from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether the user has Stay away and the product will stop displaying.

262 In this way, multiple products can be given for users to choose at one time, thereby improving sales efficiency. After selection, if the provided goods are not taken out from the shelf, the drone can take back some or all of the provided goods, thus making Users can refuse to accept defective or unsatisfactory goods, avoiding the problem of being forced to accept defective or unsatisfactory goods.

### [0031]

269 In one embodiment, dynamic images are used to display the goods.

270 In one embodiment, click on the dynamic image to select the item.

271 In one of the embodiments, several dynamic images are clicked within a preset time period, and several products corresponding to the several dynamic images are selected.

273 For example, a drone vending method includes the following steps: determine whether a user approaches, and if so, use static pictures and/or dynamic images to display the goods; click on a static picture to select a product corresponding to the static picture or click Choose a product through a dynamic image or click on a certain dynamic image to select a product corresponding to the dynamic image or click on several dynamic images during a preset time period to select several products corresponding to the several dynamic images; further determine whether the handheld terminal enters the preparatory payment state, yes Then provide the goods on the shelf according to the user's choice; further determine whether to take out the provided goods from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether the user has moved away, and if so, stop displaying the goods.

282 In this way, more complete and clearer information can be provided, and targeted advertising effects can be achieved to a certain extent.

### [0032]

287 In one embodiment, the goods are displayed in the goods area. For example, it is determined whether the user approaches, and if so, the goods are displayed in the goods area.

289 For example, use a certain area of the unmanned vending machine as the product area and display the

products in the product area. For another example, the products are displayed on a display screen of an unmanned vending machine, such as a liquid crystal display screen. In other words, the goods can be displayed in real form, or only virtual pictures or text can be given to display the goods. For example, a drone vending method includes the following steps: determine whether the user is approaching, and if so, display the goods in the goods area; further determine whether the handheld terminal enters the payment preparation state, and if so, provide the goods on the shelf according to the user's choice goods; further determine whether to take out the provided goods from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether the user has moved away, and if so, stop displaying the goods. For example, the deduction is completed based on the selling price of one item taken out from the shelf, or the deduction is completed based on the total selling price of multiple items taken out from the shelf.

[0033]

303 For example, after the goods are displayed in the goods area and before it is further determined whether the handheld terminal enters the payment preparation state, a step is also included: selecting goods from the goods area.

306 For example, a drone vending method includes the following steps: determine whether the user is approaching, and if so, display the goods in the goods area; select the goods from the goods area; further determine whether the handheld terminal enters the ready payment state, and if so, according to the user Choose to provide the goods on the shelf; further determine whether to take out the provided goods from the shelf, and if so, complete the deduction based on the selling price of the provided goods; determine whether the user has moved away, and if so, stop displaying the goods. In one embodiment, thermal induction is used to select items from the item area. For example, users can select products from the product area by touching or approaching the product area with their fingers or palms. For example, a drone vending method includes the following steps: determine whether the user is approaching, and if so, display the goods in the goods area; use thermal induction to select goods from the goods area; further determine whether the handheld terminal enters the payment preparation state, If it is, the goods will be provided on the shelf according to the user's choice; if it is further judged whether to take out the provided goods from the shelf, if it is, the deduction will be completed based on the selling price of the provided goods; if it is judged whether the user has moved away, if so, the display of the goods will be stopped. In one embodiment, infrared sensing is used to select goods from the goods area. In one embodiment, a temperature sensing method is used to select items from the item area.

[0034]

325 In one embodiment, gravity sensing is used to select items from the item area.

326 For example, the user selects goods from the goods area by pressing or stepping. For example, a drone vending method includes the following steps: determine whether the user is approaching, and if so, display the goods in the goods area; use gravity sensing to select goods from the goods area; further determine whether the handheld terminal enters the payment preparation state, If it is, the goods will be provided on the shelf according to the user's choice; if it is further judged whether to take out the provided goods from the shelf, if it is, the deduction will be completed based on the selling price of the provided goods; if it is judged

whether the user has moved away, if so, the display of the goods will be stopped.

[0035]

336 The above drone vending method can also sense or read the handheld terminal, and select goods from the goods area through a variety of methods. It is easy and flexible to use. While protecting the rights of users, it can also protect the rights of drone cargo owners, rights and interests, to achieve a win-win balance for both parties, and is especially suitable for supporting projects related to the Belt and Road construction.

[0036]

343 One example is that the drone is provided with a waiting area and/or a sales area; for example, when in use, the user enters the sales area from the outside; for example, enters the sales area from the waiting area; another example is that the sales area is open, semi-open or closed setting; for example, determine whether the user approaches, specifically determine whether the user approaches the waiting area and/or sales area; for example, determine whether the user approaches the waiting area, and if so, display the goods; another example, Determine whether the user is close to the sales area, and if so, display the goods; for example, determine whether the handheld terminal enters the pre-payment state, and if so, allow the user to enter the sales area, and provide goods on the shelf according to the user's selection; for example, the goods area setting In the sales area; for example, after determining whether the handheld terminal enters the pre-payment state, and before providing goods on the shelf according to the user's selection, it also includes the steps of: sending a request to obtain the user's video permission; when the request to obtain the user's video permission is When passed, the user is allowed to enter the sales area; the video of the user in the sales area is obtained; after the user enters the sales area, goods are provided on the shelf according to the user's choice.

356 For example, a drone vending method includes the following steps: determine whether the user is approaching, and if so, display the goods; further determine whether the handheld terminal enters the payment preparation state, and if so, send a request to obtain the user's video permission; when obtaining the user When the video permission request is passed, the user is allowed to enter the sales area; the user's video in the sales area is obtained; goods are provided on the shelf according to the user's choice; further it is judged whether to take out the provided goods from the shelf, and if so, the goods are provided based on the user's choice. The sales price is deducted; it is determined whether the user is away, and if so, the display of the goods will be stopped.

364 For another example, completing the deduction based on the selling price of the provided goods specifically includes the following steps: when the user leaves the sales area, determine whether an abnormal operation occurs based on the video, otherwise, complete the deduction based on the selling price of the provided goods. In one embodiment, it is determined based on the video whether an abnormal operation occurs, and if so, an alarm signal is issued. For example, an alarm signal is sent to the monitoring room or management area to remind managers to handle it; another example is to send an alarm signal to the sales area to remind users to stop abnormal operations; another example is to send alarm information to managers or police officers. In one embodiment, the abnormal operation includes malicious damage or destruction behavior. In one of the embodiments, the method further includes the following steps: when the user is in the sales area, determine whether an abnormal operation occurs based on the video, and if so, send an alarm signal. In one

Petitioner Exhibit 1002-4060

embodiment, the method further includes the following steps: when the user is in the sales area, determine whether an abnormality occurs based on the video, and if so, send a help signal. For example, when the user is unwell, it can be handled in time, such as rescuing the user in time. In this way, it reflects better humanistic care and improves the safety factor of drones.

[0037]

381 In one embodiment, a body-worn video device is used to obtain videos of users in the sales area.  
382 For example, the user's mobile phone is used to wirelessly connect to the server to obtain the video of the user in the sales area. For another example, when the user is allowed to enter the sales area, the user is provided with a portable video device. The portable video device includes a wearable device and a number of cameras installed on the wearable device to obtain at least three views of the user in the sales area. Videos from various angles, including videos in front of the user, behind the user, and in front of the user including parts of the user. In one embodiment, a fixed video device installed in the sales area is used to obtain the user's video in the sales area. In one embodiment, when a user is allowed to enter the sales area, a positioning tag is set for the user; when a video of the user in the sales area is obtained, a video of the user in the sales area is obtained based on the positioning tag. For example, the positioning tag is a mobile phone that confirms the mobile phone identification code or its mobile phone identification code.

[0038]

395 In one embodiment, only one user is allowed into the vending area at a time.  
396 In this case, the user is required to come out of the sales area within a certain time. The following embodiments optimize this design. In one of the embodiments, after the user is allowed to enter the sales area, the following steps are also performed simultaneously: starting a timer; and prompting the user to leave the sales area after a certain period of time. In this way, the time when users enter the store can be controlled. In one of the embodiments, it is determined whether any user among several users enters the prepayment state, and if so, all users are allowed to enter the sales area. In this way, local tyrants can bring their friends into the sales area, and parents can bring their children into the sales area. One person pays the bill and everyone benefits. For another example, when or after all users enter the sales area, steps are also executed simultaneously: start timing; and prompt users to leave the sales area after a certain period of time. In one embodiment, after allowing the user to enter the sales area, the step further includes: starting a timer; and prompting the user to leave the sales area after a certain period of time. For example, the certain time period is 1 minute, 5 minutes or 10 minutes, depending on the quantity of drone goods, and the cargo owner can also customize the certain time period, thus facilitating the cargo owner's time management and control.

[0039]

412 An example is that after completing the deduction based on the selling price of the goods provided, it also includes the step of sending information about the goods that were deducted, for example, to a preset terminal or server, so that the owner of the goods can clearly know the sales status of the goods.  
415 Another example is sending information about deducted goods regularly; for example, sending it once an

hour, or once a day, and so on. For example, when sending information about deducted goods, the identity information of the drone where the goods are located is attached. For example, the identity information is the serial number or serial number of the drone; in this way, it is helpful for the cargo owner to manage multiple drones. .

[0040]

423 It should be noted that other embodiments of the present invention also include an implementable drone vending method formed by combining the technical features in the above embodiments.

[0041]

428 The technical features of the above-described embodiments can be combined in any way. To simplify the description, not all possible combinations of the technical features in the above-described embodiments are described. However, as long as there is no contradiction in the combination of these technical features, All should be considered to be within the scope of this manual.

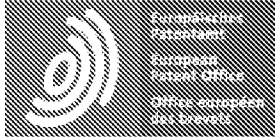
[0042]

435 The above-mentioned embodiments only express several implementation modes of the present invention. The descriptions are relatively specific and detailed, but they should not be construed as limiting the scope of the invention.

438 It should be noted that, for those of ordinary skill in the art, several modifications and improvements can be made without departing from the concept of the present invention, and these all belong to the protection scope of the present invention.

441 Therefore, the scope of protection of the patent of the present invention should be determined by the appended claims.





## Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

### CLAIMS CN107480975A

1.

*13* A drone vending method is characterized by including the following steps:

*14* Determine whether the user is approaching, and if so, display the product;

*15* It is further determined whether the handheld terminal has entered the payment preparation state, and if so, the goods will be provided on the shelf according to the user's choice;

*17* Further determine whether to take out the provided goods from the shelf, and if so, complete the deduction based on the selling price of the provided goods;

*19* Determine whether the user has moved away, and if so, stop displaying the goods.

2.

*23* The drone vending method according to claim 1, characterized in that the handheld terminal scans the code to enter the preparatory payment state.

3.

*28* The drone vending method according to claim 2, characterized in that the handheld terminal scans the QR code or barcode to enter the preparatory payment state.

4.

*33* The drone vending method according to claim 1, characterized in that the proximity sensing handheld terminal enters a preparatory payment state.

5.

38 The drone vending method according to claim 4, characterized in that NFC or RFID short-range sensing handheld terminal is used to enter the preparatory payment state.

6.

43 The drone vending method according to claim 1, characterized in that the goods are displayed in the goods area.

7.

48 The drone vending method according to claim 6, characterized in that a thermal induction method is used to select goods from the goods area.

8.

53 The drone vending method according to claim 7, characterized in that infrared sensing is used to select goods from the goods area.

9.

58 The drone vending method according to claim 7, characterized in that a temperature sensing method is used to select goods from the goods area.

10.

63 The drone vending method according to claim 6, characterized in that a gravity sensing method is used to select goods from the goods area.



(12)发明专利申请

(10)申请公布号 CN 107480975 A

(43)申请公布日 2017.12.15

(21)申请号 201710623807.4

(22)申请日 2017.07.27

(71)申请人 惠州市伊涅科技有限公司  
地址 516000 广东省惠州市博罗县龙溪镇  
龙溪大道13号

(72)发明人 温玉桂

(74)专利代理机构 广州华进联合专利商标代理  
有限公司 44224

代理人 邓云鹏

(51)Int.Cl.

G06Q 20/18(2012.01)

G06Q 20/32(2012.01)

G07F 9/02(2006.01)

G07F 11/00(2006.01)

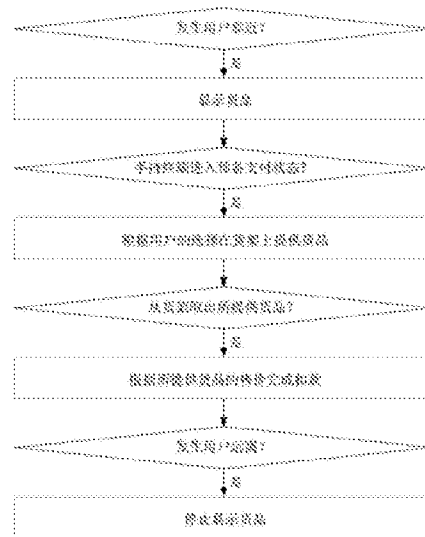
权利要求书1页 说明书6页 附图1页

(54)发明名称

无人机售货方法

(57)摘要

本发明涉及一种无人机售货方法,其包括以下步骤:判断是否发生用户靠近,是则显示货品;进一步判断手持终端是否进入预备支付状态,是则根据用户的选择在货架上提供货品;进一步判断是否从货架取出所提供货品,是则根据所提供货品的售价完成扣款;判断是否发生用户远离,是则停止显示货品。上述无人机售货方法,当用户靠近时才显示货品,在用户远离后则停止显示货品,无需不断地照明造成能源浪费,并且避免了被展示货品长期被日晒容易被氧化,使得货品保质期更长,且仅当用户从货架取出所提供货品才完成扣款,给用户提供了更自由的选择权利,特别适合一带一路建设的相关工程配套使用。



CN 107480975 A

1. 一种无人机售货方法,其特征在于,包括以下步骤:  
判断是否发生用户靠近,是则显示货品;  
进一步判断手持终端是否进入预备支付状态,是则根据用户的选择在货架上提供货品;  
进一步判断是否从货架取出所提供货品,是则根据所提供货品的售价完成扣款;  
判断是否发生用户远离,是则停止显示货品。
2. 根据权利要求1所述无人机售货方法,其特征在于,手持终端扫码进入预备支付状态。
3. 根据权利要求2所述无人机售货方法,其特征在于,手持终端扫二维码或条形码进入预备支付状态。
4. 根据权利要求1所述无人机售货方法,其特征在于,近距感应手持终端进入预备支付状态。
5. 根据权利要求4所述无人机售货方法,其特征在于,采用NFC或RFID近距感应手持终端进入预备支付状态。
6. 根据权利要求1所述无人机售货方法,其特征在于,在货品区域显示货品。
7. 根据权利要求6所述无人机售货方法,其特征在于,采用热感应方式从货品区域选择货品。
8. 根据权利要求7所述无人机售货方法,其特征在于,采用红外感应方式从货品区域选择货品。
9. 根据权利要求7所述无人机售货方法,其特征在于,采用温度感应方式从货品区域选择货品。
10. 根据权利要求6所述无人机售货方法,其特征在于,采用重力感应方式从货品区域选择货品。

## 无人机售货方法

### 技术领域

[0001] 本发明涉及无人售货领域,特别是涉及无人机售货方法。

### 背景技术

[0002] 现有的自动售货无人机(亦称:无人自动售货机,简称:无人机),常用于商场、公园、景区及游乐场所等,能够节约人力资源。

[0003] 但是,自动售货无人机往往需要不断地照明,尤其是长期无人时还要继续照明,造成能源浪费,看得人心痛,不利于与时俱进地建设绿色节能型的可持续发展新中国,并且,自动售货无人机中被展示的货品长期被日晒,容易被氧化。

### 发明内容

[0004] 基于此,有必要针对如何改进自动售货无人机往往需要不断地照明造成能源浪费以及自动售货无人机中被展示货品长期被日晒容易被氧化的问题,提供一种无人机售货方法。

[0005] 一种无人机售货方法,其包括以下步骤:判断是否发生用户靠近,是则显示货品;进一步判断手持终端是否进入预备支付状态,是则根据用户的选择在货架上提供货品;进一步判断是否从货架取出所提供货品,是则根据所提供货品的售价完成扣款;判断是否发生用户远离,是则停止显示货品。

[0006] 上述无人机售货方法,当用户靠近时才显示货品,在用户远离后则停止显示货品,无需不断地照明造成能源浪费,并且避免了被展示货品长期被日晒容易被氧化,使得货品保质期更长,且仅当用户从货架取出所提供货品才完成扣款,给用户提供了更自由的选择权利,特别适合一带一路建设的相关工程配套使用。

[0007] 在其中一个实施例中,手持终端扫码进入预备支付状态。

[0008] 在其中一个实施例中,手持终端扫二维码或条形码进入预备支付状态。

[0009] 在其中一个实施例中,近距感应手持终端进入预备支付状态。

[0010] 在其中一个实施例中,采用NFC或RFID近距感应手持终端进入预备支付状态。

[0011] 在其中一个实施例中,在货品区域显示货品。

[0012] 在其中一个实施例中,采用热感应方式从货品区域选择货品。

[0013] 在其中一个实施例中,采用红外感应方式从货品区域选择货品。

[0014] 在其中一个实施例中,采用温度感应方式从货品区域选择货品。

[0015] 在其中一个实施例中,采用重力感应方式从货品区域选择货品。

[0016] 上述无人机售货方法,还能够对手持终端进行感应或读取,以及通过多种方式从货品区域选择货品,使用方便、灵活,在保障用户权利的同时,也能够保障无人机货主的权益,达到双方共赢的平衡,特别适合一带一路建设的相关工程配套使用。

### 附图说明

[0017] 图1为本发明的一实施例的示意图。

### 具体实施方式

[0018] 为使本发明的上述目的、特征和优点能够更加明显易懂，下面结合附图对本发明的具体实施方式做详细的说明。在下面的描述中阐述了很多具体细节以便于充分理解本发明。但是本发明能够以很多不同于在此描述的其它方式来实施，本领域技术人员可以在不违背本发明内涵的情况下做类似改进，因此本发明不受下面公开的具体实施例的限制。

[0019] 需要说明的是，当元件被称为“固定于”或“设置于”另一个元件，它可以直接在另一个元件上或者也可以存在居中的元件。当一个元件被认为是“连接”另一个元件，它可以是直接连接到另一个元件或者可能同时存在居中元件。本文所使用的术语“垂直的”、“水平的”、“左”、“右”以及类似的表述只是为了说明的目的，并不表示是唯一的实施方式。

[0020] 除非另有定义，本文所使用的所有的技术和科学术语与属于本发明的技术领域的技术人员通常理解的含义相同。本文所使用的术语只是为了描述具体的实施方式的目的，不是旨在于限制本发明。本文所使用的术语“和/或”包括一个或多个相关的所列项目的任意的和所有的组合。

[0021] 如图1所示，本发明一个实施例是，一种无人机售货方法，应用于无人自动售货机，所述无人机售货方法包括以下步骤：判断是否发生用户靠近，是则显示货品；进一步判断手持终端是否进入预备支付状态，是则根据用户的选择在货架上提供货品；进一步判断是否从货架取出所提供货品，是则根据所提供货品的售价完成扣款；判断是否发生用户远离，是则停止显示货品。上述无人机售货方法，当用户靠近时才显示货品，在用户远离后则停止显示货品，无需不断地照明造成能源浪费，并且避免了被展示货品长期被日晒容易被氧化，使得货品保质期更长，且仅当用户从货架取出所提供货品才完成扣款，给用户提供了更自由的选择权利，特别适合一带一路建设的相关工程配套使用。

[0022] 例如，无人机售货方法中，判断是否发生用户靠近，是则显示货品，否则不执行任何操作，即无需显示货品；例如，无人机售货方法中，进一步判断手持终端是否进入预备支付状态，是则根据用户的选择在货架上提供货品，否则不执行任何操作，即无需在货架上提供货品；例如，无人机售货方法中，进一步判断是否从货架取出所提供货品，是则根据所提供货品的售价完成扣款，否则不执行任何操作，即无需执行扣款操作；例如，无人机售货方法中，判断是否发生用户远离，是则停止显示货品，否则保持当前界面，例如显示货品或者根据用户的选择在货架上提供货品等。

[0023] 在其中一个实施例中，手持终端扫码进入预备支付状态。例如，一种无人机售货方法，其包括以下步骤：判断是否发生用户靠近，是则显示货品；进一步判断手持终端是否通过扫码进入预备支付状态，是则根据用户的选择在货架上提供货品；进一步判断是否从货架取出所提供货品，是则根据所提供货品的售价完成扣款；判断是否发生用户远离，是则停止显示货品。例如，用户拿着手机扫码进入预备支付状态。在其中一个实施例中，手持终端扫二维码或条形码进入预备支付状态。在其中一个实施例中，近距感应手持终端进入预备支付状态。例如，一种无人机售货方法，其包括以下步骤：判断是否发生用户靠近，是则显示货品；进一步判断手持终端是否通过近距感应进入预备支付状态，是则根据用户的选择在货架上提供货品；进一步判断是否从货架取出所提供货品，是则根据所提供货品的售价完

成扣款；判断是否发生用户远离，是则停止显示货品。例如，用户拿着手机近距离感应，进入预备支付状态。在其中一个实施例中，采用NFC或RFID近距离感应手持终端进入预备支付状态。这样，只需手持终端即可进入预备支付状态。

[0024] 一个例子是，将所述预备支付状态与用户的身份信息（例如身份证号）相关联，由于用户的身份信息往往是唯一的，因此对应的用户也是唯一的，这样可以更好地确保收款情况。例如，确定手持终端进入预备支付状态之后，根据用户的选择在货架上提供货品之前，还包括步骤：将所述预备支付状态与用户的身份信息相关联，根据用户的历史成交记录判断用户的支付信用是否满足一定信用阈值，是则执行后续步骤；即根据用户的历史成交记录确定其支付信用满足一定信用阈值时，然后再根据用户的选择在货架上提供货品，或者，确定进入预备支付状态之后，所述根据用户的选择在货架上提供货品具体包括以下步骤：所述预备支付状态与用户的身份信息相关联，根据用户的历史成交记录确定其支付信用满足一定信用阈值时，根据用户的选择在货架上提供货品；其中，信用阈值可根据经验、银行信用及/或社会征信等灵活设置。例如，在确定用户的选择（即用户选择货品）之后，在货架上提供货品之前，还包括步骤：根据所述预备支付状态查询用户的支付能力，在支付能力满足所选择货品时，则执行后续步骤，即在用户支付能力满足其选择时在货架上提供货品。这样，可以避免用户故意透支消费，也可以避免用户非主观恶意透支消费，特别是非完全行为能力人的无法自控的面子消费等，从而有利于维护用户利益，正确引导用户的合理消费，从而有力地维护了社会正常秩序。

[0025] 在其中一个实施例中，采用静态图片显示货品，例如采用多个静态图片显示多个货品或者采用多个静态图片显示一个货品或者采用一个静态图片显示一个货品。在其中一个实施例中，显示货品之后，根据用户的选择在货架上提供货品之前，还包括步骤：点击静态图片选择货品。例如，进一步判断手持终端是否进入预备支付状态之前或之后，点击静态图片选择货品，然后在手持终端进入预备支付状态时或之后，根据用户的选择在货架上提供货品。例如，一种无人机售货方法，其包括以下步骤：判断是否发生用户靠近，是则采用静态图片显示货品；点击静态图片选择货品；进一步判断手持终端是否进入预备支付状态，是则根据用户的选择在货架上提供货品；进一步判断是否从货架取出所提供货品，是则根据所提供货品的售价完成扣款；判断是否发生用户远离，是则停止显示货品。在其中一个实施例中，点击某一静态图片选择该静态图片对应的一货品。在其中一个实施例中，在预设时间段点击若干静态图片，选择该若干静态图片分别对应的若干货品。例如，一种无人机售货方法，其包括以下步骤：判断是否发生用户靠近，是则采用静态图片显示货品；点击某一静态图片选择该静态图片对应的一货品；进一步判断手持终端是否进入预备支付状态，是则根据用户的选择在货架上提供货品；进一步判断是否从货架取出所提供货品，是则根据所提供货品的售价完成扣款；判断是否发生用户远离，是则停止显示货品。例如，一种无人机售货方法，其包括以下步骤：判断是否发生用户靠近，是则采用静态图片显示货品；在预设时间段点击若干静态图片，选择该若干静态图片分别对应的若干货品；进一步判断手持终端是否进入预备支付状态，是则根据用户的选择在货架上提供货品；进一步判断是否从货架取出所提供货品，是则根据所提供货品的售价完成扣款；判断是否发生用户远离，是则停止显示货品。这样，可以一次给出多个货品以供用户选择，从而提高了销售效率，还在选择之后，如果没有从货架取出所提供货品，则无人机可以收回部分或全部所提供的货品，从而使

得用户可以拒绝接受瑕疵品或不满意货品,避免了被迫接受瑕疵品或不满意货品的问题。

[0026] 在其中一个实施例中,采用动态图像显示货品。在其中一个实施例中,点击动态图像选择货品。在其中一个实施例中,在预设时间段点击若干动态图像,选择该若干动态图像分别对应的若干货品。例如,一种无人售货方法,其包括以下步骤:判断是否发生用户靠近,是则采用静态图片及/或动态图像显示货品;点击某一静态图片选择该静态图片对应的一货品或点击动态图像选择货品或点击某一动态图像选择该动态图像对应的一货品或在预设时间段点击若干动态图像选择该若干动态图像分别对应的若干货品;进一步判断手持终端是否进入预备支付状态,是则根据用户的选择在货架上提供货品;进一步判断是否从货架取出所提供货品,是则根据所提供货品的售价完成扣款;判断是否发生用户远离,是则停止显示货品。这样,可以提供更完善更清晰的信息,也可以在一定程度上实现定点广告效果。

[0027] 在其中一个实施例中,在货品区域显示货品,例如,判断是否发生用户靠近,是则在货品区域显示货品。例如,以无人售货机的某一区域作为货品区域,在货品区域显示货品。又如,在无人售货机的显示屏例如液晶显示屏显示货品。也就是说,可以真实给出货品来进行显示,也可以只给出虚拟的图片或者文字来显示货品。例如,一种无人售货方法,其包括以下步骤:判断是否发生用户靠近,是则在货品区域显示货品;进一步判断手持终端是否进入预备支付状态,是则根据用户的选择在货架上提供货品;进一步判断是否从货架取出所提供货品,是则根据所提供货品的售价完成扣款;判断是否发生用户远离,是则停止显示货品。例如,根据从货架取出所提供的一个货品的售价完成扣款,或者,根据从货架取出所提供的多个货品的总售价完成扣款。

[0028] 例如,在货品区域显示货品之后,以及进一步判断手持终端是否进入预备支付状态之前,还包括步骤:从货品区域选择货品。例如,一种无人售货方法,其包括以下步骤:判断是否发生用户靠近,是则在货品区域显示货品;从货品区域选择货品;进一步判断手持终端是否进入预备支付状态,是则根据用户的选择在货架上提供货品;进一步判断是否从货架取出所提供货品,是则根据所提供货品的售价完成扣款;判断是否发生用户远离,是则停止显示货品。在其中一个实施例中,采用热感应方式从货品区域选择货品。例如,用户用手指或手掌触碰或贴近货品区域,即可从货品区域选择货品。例如,一种无人售货方法,其包括以下步骤:判断是否发生用户靠近,是则在货品区域显示货品;采用热感应方式从货品区域选择货品;进一步判断手持终端是否进入预备支付状态,是则根据用户的选择在货架上提供货品;进一步判断是否从货架取出所提供货品,是则根据所提供货品的售价完成扣款;判断是否发生用户远离,是则停止显示货品。在其中一个实施例中,采用红外感应方式从货品区域选择货品。在其中一个实施例中,采用温度感应方式从货品区域选择货品。

[0029] 在其中一个实施例中,采用重力感应方式从货品区域选择货品。例如,用户采用压触或者踩踏方式从货品区域选择货品。例如,一种无人售货方法,其包括以下步骤:判断是否发生用户靠近,是则在货品区域显示货品;采用重力感应方式从货品区域选择货品;进一步判断手持终端是否进入预备支付状态,是则根据用户的选择在货架上提供货品;进一步判断是否从货架取出所提供货品,是则根据所提供货品的售价完成扣款;判断是否发生用户远离,是则停止显示货品。

[0030] 上述无人售货方法,还能够对手持终端进行感应或读取,以及通过多种方式从



货品区域选择货品,使用方便、灵活,在保障用户权利的同时,也能够保障无人机货主的权益,达到双方共赢的平衡,特别适合一带一路建设的相关工程配套使用。

[0031] 一个例子是,所述无人机设置有等待区及/或售货区;例如,使用时,用户从外部进入售货区;例如,从等待区进入售货区;又如,售货区开放、半开放或者封闭式设置;例如,判断是否发生用户靠近,具体为判断是否发生用户靠近等待区及/或售货区;例如,判断是否发生用户靠近等待区,是则显示货品;又如,判断是否发生用户靠近售货区,是则显示货品;例如,判断手持终端是否进入预备支付状态,是则允许用户进入售货区,根据用户的选择在货架上提供货品;例如所述货品区域设置于所述售货区;例如,判断手持终端是否进入预备支付状态之后,根据用户的选择在货架上提供货品之前,还包括步骤:发送获取用户视频权限的请求;当获取用户视频权限的请求被通过时,允许用户进入售货区;获取用户在售货区的视频;在用户进入售货区之后,再根据用户的选择在货架上提供货品。例如,一种无人机售货方法,其包括以下步骤:判断是否发生用户靠近,是则显示货品;进一步判断手持终端是否进入预备支付状态,是则发送获取用户视频权限的请求;当获取用户视频权限的请求被通过时,允许用户进入售货区;获取用户在售货区的视频;根据用户的选择在货架上提供货品;进一步判断是否从货架取出所提供货品,是则根据所提供货品的售价完成扣款;判断是否发生用户远离,是则停止显示货品。又如,根据所提供货品的售价完成扣款,具体包括以下步骤:当用户离开售货区时,根据所述视频判断是否发生异常操作,否则根据所提供货品的售价完成扣款。在其中一个实施例中,根据所述视频判断是否发生异常操作,是则发出报警信号。例如,向监控室或者管理区发出报警信号,以提醒管理人员进行处理;又如,在售货区发出报警信号,以提醒用户停止异常操作;又如,向管理人员或者警务人员发送报警信息。在其中一个实施例中,所述异常操作包括恶意的损毁或破坏行为。在其中一个实施例中,还包括以下步骤:当用户处于售货区时,根据所述视频判断是否发生异常操作,是则发出报警信号。在其中一个实施例中,还包括以下步骤:当用户处于售货区时,根据所述视频判断是否发生异常状况,是则发出求助信号。例如,当用户身体不适时,能够及时处理,例如及时抢救用户。这样,体现了更好的人文关怀,提升了无人机的安全系数。

[0032] 在其中一个实施例中,采用随身视频设备获取用户在售货区的视频。例如,采用用户的手机无线连接服务器以获取用户在售货区的视频。又如,允许用户进入售货区时,为用户提供随身视频设备,所述随身视频设备包括可穿戴设备,以及安装于可穿戴设备上的若干摄像头,用于获取用户在售货区的至少三个角度的视频,包括用户前方、用户后方以及包含有用户部分的用户前方的视频。在其中一个实施例中,采用在售货区安装的固定视频设备获取用户在售货区的视频。在其中一个实施例中,允许用户进入售货区时,为用户设置定位标签;获取用户在售货区的视频时,根据所述定位标签获取用户在售货区的视频。例如,所述定位标签为确认手机识别码的手机或其手机识别码。

[0033] 在其中一个实施例中,每次仅允许一个用户进入售货区。这种情况下,要求用户在一定时间从售货区出来,下面的实施例对此进行了优化设计。在其中一个实施例中,允许用户进入售货区之后,还同步执行步骤:开始计时;并且在达到一定时长之后提示用户离开售货区。这样,可以控制用户进店时间。在其中一个实施例中,判断若干用户中是否任一用户进入预备支付状态,是则允许全部用户进入售货区。这样,土豪可以带着伙伴们一起进入售货区,家长可以带着孩子一起进入售货区,一人买单,全体受益。又如,全部用户进入售货区

时或之后,还同步执行步骤:开始计时;并且在达到一定时长之后提示用户离开售货区。在其中一个实施例中,允许用户进入售货区之后,还包括步骤:开始计时;并且在达到一定时长之后提示用户离开售货区。例如,所述一定时长为1分钟、5分钟或10分钟,根据无人机货品数量而定,货主也可以自定义该一定时长,从而方便了货主的时间管控。

[0034] 一个例子是,根据所提供货品的售价完成扣款之后,还包括步骤:发送被扣款的货品的信息,例如发送到预设终端或者服务器,这样,货主可以清楚地知道货品售卖情况。又如,定时发送被扣款的货品的信息;例如,每小时发送一次,或者每天发送一次,以此类推。例如,发送被扣款的货品的信息时,附加货品所在的无人机的身份信息,例如,所述身份信息是无人机的编号或者序列号;这样,有利于货主管理多个无人机。

[0035] 需要说明的是,本发明的其它实施例还包括,上述各实施例中的技术特征相互组合所形成的、能够实施的无人机售货方法。

[0036] 以上所述实施例的各技术特征可以进行任意的组合,为使描述简洁,未对上述实施例中的各个技术特征所有可能的组合都进行描述,然而,只要这些技术特征的组合不存在矛盾,都应当认为是本说明书记载的范围。

[0037] 以上所述实施例仅表达了本发明的几种实施方式,其描述较为具体和详细,但不能因此而理解为对发明专利范围的限制。应当指出的是,对于本领域的普通技术人员来说,在不脱离本发明构思的前提下,还可以做出若干变形和改进,这些都属于本发明的保护范围。因此,本发明的保护范围应以所附权利要求为准。

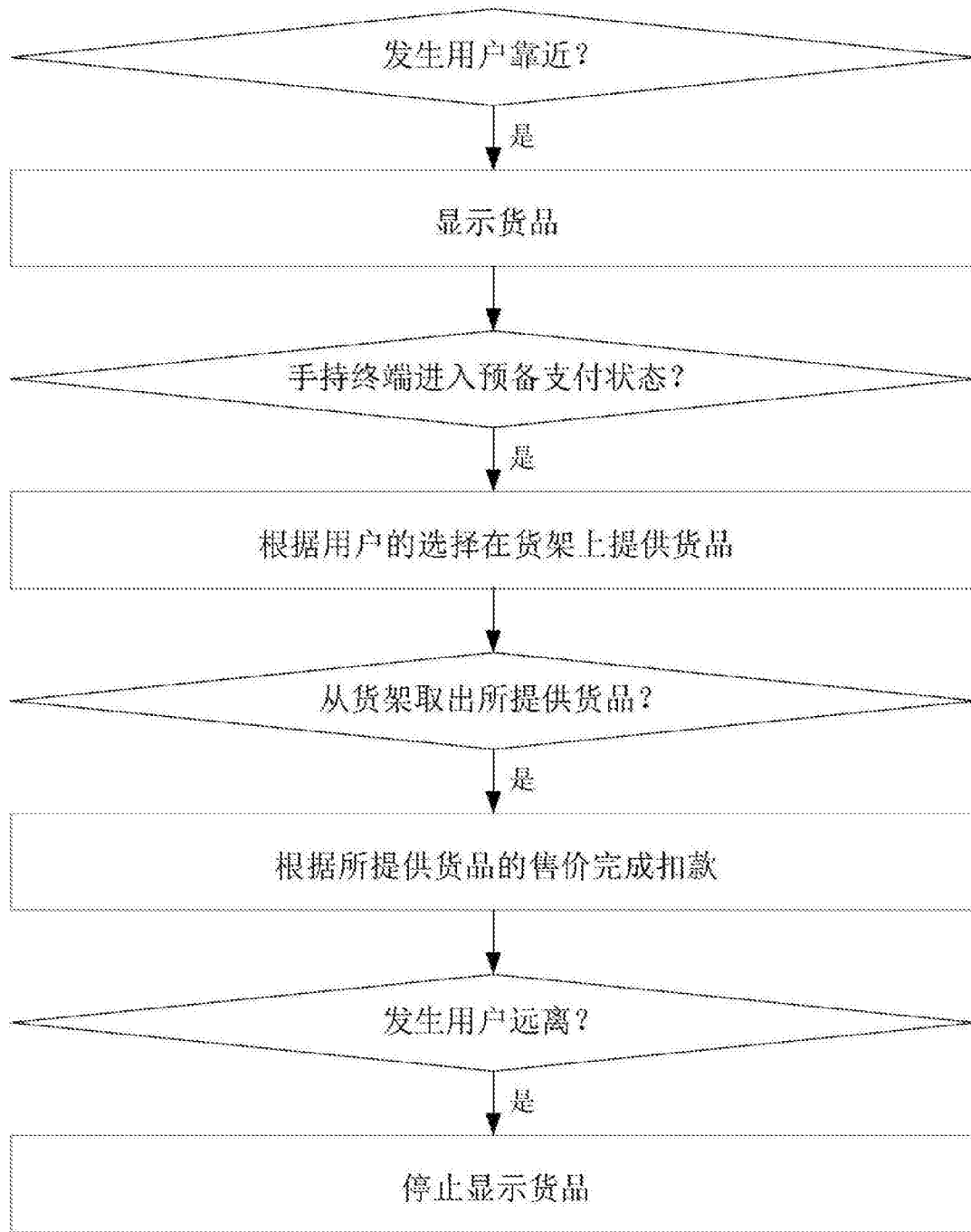


图1



UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

24341 7590 09/16/2022
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

Table with 2 columns: EXAMINER (POINVIL, FRANTZY), ART UNIT (3698), PAPER NUMBER

DATE MAILED: 09/16/2022

Table with 5 columns: APPLICATION NO. (17/654,732), FILING DATE (03/14/2022), FIRST NAMED INVENTOR (Paresh K. Patel), ATTORNEY DOCKET NO. (104402-5065-US), CONFIRMATION NO. (5715)

TITLE OF INVENTION: METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Table with 7 columns: APPLN. TYPE (nonprovisional), ENTITY STATUS (SMALL), ISSUE FEE DUE (\$600), PUBLICATION FEE DUE (\$0.00), PREV. PAID ISSUE FEE (\$0.00), TOTAL FEE(S) DUE (\$600), DATE DUE (12/16/2022)

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies. If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above. If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)". For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

**PART B - FEE(S) TRANSMITTAL**

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: **Mail Stop ISSUE FEE**  
**Commissioner for Patents**  
**P.O. Box 1450**  
**Alexandria, Virginia 22313-1450**

By fax, send to: **(571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the **ISSUE FEE** and **PUBLICATION FEE** (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

24341                      7590                      09/16/2022  
**Morgan, Lewis & Bockius LLP (PA)**  
**1400 Page Mill Road**  
**Palo Alto, CA 94304-1124**

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/654,732	03/14/2022	Paresh K. Patel	104402-5065-US	5715

TITLE OF INVENTION: **METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS**

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$600	\$0.00	\$0.00	\$600	12/16/2022

EXAMINER	ART UNIT	CLASS-SUBCLASS
POINVIL, FRANTZY	3698	705-044000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.</p> <p><input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. <b>Use of a Customer Number is required.</b></p>	<p>2. For printing on the patent front page, list</p> <p>(1) The names of up to 3 registered patent attorneys or agents OR, alternatively, _____ 1</p> <p>(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. _____ 2</p> <p>_____ 3</p>
--	---

**3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)**

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE \_\_\_\_\_ (B) RESIDENCE: (CITY and STATE OR COUNTRY) \_\_\_\_\_

Please check the appropriate assignee category or categories (will not be printed on the patent) :  Individual  Corporation or other private group entity  Government

4a. Fees submitted:  Issue Fee  Publication Fee (if required)  Advance Order - # of Copies \_\_\_\_\_

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

Electronic Payment via EFS-Web  Enclosed check  Non-electronic payment by credit card (Attach form PTO-2038)

The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. \_\_\_\_\_

**5. Change in Entity Status** (from status indicated above)

Applicant certifying micro entity status. See 37 CFR 1.29

Applicant asserting small entity status. See 37 CFR 1.27

Applicant changing to regular undiscounted fee status.

**NOTE:** Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

**NOTE:** If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

**NOTE:** Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

**NOTE:** This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature \_\_\_\_\_ Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_ Registration No. \_\_\_\_\_

**Petitioner Exhibit 1002-4075**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes application details for Paresh K. Patel and examiner information for POINVIL, FRANTZY.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

## OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

### Privacy Act Statement

**The Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

<b>Notice of Allowability</b>	<b>Application No.</b> 17/654,732	<b>Applicant(s)</b> Patel, Paresh K.	
	<b>Examiner</b> FRANTZY POINVIL	<b>Art Unit</b> 3698	<b>AIA (FITF) Status</b> Yes

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.  This communication is responsive to the response filed 8/19/2022.  
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on \_\_\_\_\_.
2.  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
3.  The allowed claim(s) is/are 1-20. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/pph/index.jsp](http://www.uspto.gov/patents/init_events/pph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).
4.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

**Certified copies:**

- a)  All      b)  Some\*      c)  None of the:
1.  Certified copies of the priority documents have been received.
  2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5.  CORRECTED DRAWINGS (as "replacement sheets") must be submitted.  
 including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
6.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |   |  |
|---|--|
| 1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 5. <input type="checkbox"/> Examiner's Amendment/Comment                             |
| 2. <input checked="" type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br>Paper No./Mail Date <u>8/21/2022</u> . | 6. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| 3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material _____.               | 7. <input type="checkbox"/> Other _____.   |
| 4. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date. _____.   |  |

/FRANTZY POINVIL/  
Primary Examiner, Art Unit 3698



## **DETAILED ACTION**

### *Notice of Pre-AIA or AIA Status*

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

### **Allowable Subject**

2. The following is an examiner's statement of reasons for allowance:

Claims 1-20 are allowable over the art of record.

The prior art taken alone or in combination failed to teach or suggest:

“identifying one or more payment accepting units in proximity to the mobile device that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services, and displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input to (i) receive selection by a user of the mobile device of an available payment accepting unit of the one or more payment accepting units and (ii) trigger payment by the mobile payment application for a transaction initiated by the user of the mobile device with the available payment accepting unit of the one or more payment accepting units”, as recited in independent claims 1, 13 and 15.

3. The prior following prior art taken alone or in combination fails to teach or suggest the above noted limitations.

Mei (US 20190236586 A1) discloses a payment processing method and apparatus, where the payment processing method includes obtaining, by a payee terminal, transaction information of a payment card application, determining, by the payee terminal based on the transaction information, that a running environment of the payment card application is a mobile terminal device; and sending, by the payee terminal, payment voucher information of the payment card application to the mobile terminal device using a first communications technology, where the first communications technology includes a short range communications technology. Hence, a user can conveniently manage and view payment voucher information.

Xu et al (US 20160132870 A1) disclose a method implemented at a server to facilitate secure offline transactions. The server receives, from a client device, an authorization request that includes a user identifier, first financial account information and a secure code. The server authenticates the authorization request, and sends a first transaction approval to the client device. Then, in accordance with the information received in the authorization request, the server facilitates a secure transaction between the client device and a point-of-sale (POS) machine while the client device is offline. Specifically, the server receives, from the POS machine, a transaction request that includes at least the user identifier and the security code. The server retrieves the first financial account information from a memory according to the user identifier and the security code, performs a transaction operation associated with the first financial account information, and sends a second transaction approval to the POS machine.

The above recited limitations provide meaningful limitations that transforms the abstract idea into patent eligible. The claim as a whole effects an improvement to another technology or technical field. These limitations in combination provide meaningful limitations beyond generally linking the use of the abstract idea to a practical application.

### *Conclusion*

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to FRANTZY POINVIL whose telephone number is (571)272-6797. The examiner can normally be reached M-Th 7:00AM to 5:30PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Anderson can be reached on 571-270-0508. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: <https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent-center> for more information about Patent Center and <https://www.uspto.gov/patents/docx> for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/fp/

/FRANTZY POINVIL/  
Primary Examiner, Art Unit 3698

August 31, 2022

<b>Notice of References Cited</b>	Application/Control No. 17/654,732	Applicant(s)/Patent Under Reexamination Patel, Paresh K.	
	Examiner FRANTZY POINVIL	Art Unit 3698	Page 1 of 1

**U.S. PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20190236586-A1	08-2019	Mei; Jingqing	G06Q20/401	1/1
*	B	US-20140337235-A1	11-2014	VAN HEERDEN; Lauren	G06Q20/383	705/71
*	C	US-20080040265-A1	02-2008	Rackley III; Brady Lee	G06Q20/102	705/40
*	D	US-11074577-B1	07-2021	Soccorsy; Benjamin	G06Q20/385	1/1
*	E	US-20130282590-A1	10-2013	Rajarethnam; Rajeshwar	G06Q20/3276	705/71
*	F	US-20120203666-A1	08-2012	Torossian; Arthur	G06Q20/027	705/26.41
*	G	US-20080010193-A1	01-2008	Rackley III; Brady Lee	G06Q20/325	705/39
*	H	US-20160132870-A1	05-2016	Xu; Jiajie	G06Q20/382	705/21
	I					
	J					
	K					
	L					
	M					

**FOREIGN PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

**NON-PATENT DOCUMENTS**

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Hoffman et al., "New options in Wireless payments", Internet World 7.7:37 Penton Media Inc., Penton Business Media, Inc. and their subsidiaries . (Year: 2001).
	V	Carton et al., "Framework for Mobile Payments Integration", Electronic Journal of Information Systems Evaluation, 15.1: 13-24, Academic Conferences International Limited, January. (Year: 2012).
	W	
	X	

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.



UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

24341 7590 10/06/2022
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

Table with 2 columns: EXAMINER (POINVIL, FRANTZY), ART UNIT (3698), PAPER NUMBER

DATE MAILED: 10/06/2022

Table with 5 columns: APPLICATION NO. (17/147,305), FILING DATE (01/12/2021), FIRST NAMED INVENTOR (Paresh K. Patel), ATTORNEY DOCKET NO. (104402-5046-US), CONFIRMATION NO. (8393)

TITLE OF INVENTION: METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Table with 7 columns: APPLN. TYPE (nonprovisional), ENTITY STATUS (SMALL), ISSUE FEE DUE (\$600), PUBLICATION FEE DUE (\$0.00), PREV. PAID ISSUE FEE (\$0.00), TOTAL FEE(S) DUE (\$600), DATE DUE (01/06/2023)

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies. If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above. If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)". For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

**PART B - FEE(S) TRANSMITTAL**

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: **Mail Stop ISSUE FEE**  
**Commissioner for Patents**  
**P.O. Box 1450**  
**Alexandria, Virginia 22313-1450**

By fax, send to: **(571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the **ISSUE FEE** and **PUBLICATION FEE** (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

24341                      7590                      10/06/2022  
**Morgan, Lewis & Bockius LLP (PA)**  
**1400 Page Mill Road**  
**Palo Alto, CA 94304-1124**

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/147,305	01/12/2021	Paresh K. Patel	104402-5046-US	8393

TITLE OF INVENTION: **METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS**

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$600	\$0.00	\$0.00	\$600	01/06/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
POINVIL, FRANTZY	3698	705-044000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.
- "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively, \_\_\_\_\_ 1
- (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. \_\_\_\_\_ 2
- \_\_\_\_\_ 3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE \_\_\_\_\_ (B) RESIDENCE: (CITY and STATE OR COUNTRY) \_\_\_\_\_

Please check the appropriate assignee category or categories (will not be printed on the patent) :  Individual  Corporation or other private group entity  Government

4a. Fees submitted:  Issue Fee  Publication Fee (if required)  Advance Order - # of Copies \_\_\_\_\_

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

- Electronic Payment via EFS-Web  Enclosed check  Non-electronic payment by credit card (Attach form PTO-2038)
- The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. \_\_\_\_\_

5. Change in Entity Status (from status indicated above)

- Applicant certifying micro entity status. See 37 CFR 1.29
- Applicant asserting small entity status. See 37 CFR 1.27
- Applicant changing to regular undiscounted fee status.

**NOTE:** Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

**NOTE:** If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

**NOTE:** Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

**NOTE:** This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature \_\_\_\_\_ Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_ Registration No. \_\_\_\_\_

**Petitioner Exhibit 1002-4084**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes application details for Paresh K. Patel and examiner information for POINVIL, FRANTZY.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

## OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

### Privacy Act Statement

**The Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



<b>Notice of Allowability</b>	<b>Application No.</b> 17/147,305	<b>Applicant(s)</b> Patel, Paresh K.	
	<b>Examiner</b> FRANTZY POINVIL	<b>Art Unit</b> 3698	<b>AIA (FITF) Status</b> Yes

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.  This communication is responsive to the response filed 9/15/2022.  
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on \_\_\_\_\_.
2.  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
3.  The allowed claim(s) is/are 2-29. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/pph/index.jsp](http://www.uspto.gov/patents/init_events/pph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).
4.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

**Certified copies:**

- a)  All      b)  Some\*      c)  None of the:
1.  Certified copies of the priority documents have been received.
  2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5.  CORRECTED DRAWINGS (as "replacement sheets") must be submitted.  
 including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
6.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |   |  |
|---|--|
| 1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 5. <input type="checkbox"/> Examiner's Amendment/Comment                             |
| 2. <input checked="" type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br>Paper No./Mail Date <u>8/30/2022; 9/22/2022.</u> | 6. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| 3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material _____.                         | 7. <input checked="" type="checkbox"/> Other <u>IDS 8/17/2022.</u>                   |
| 4. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date. _____.   |  |

/FRANTZY POINVIL/  
Primary Examiner, Art Unit 3698

**DETAILED ACTION**

*Notice of Pre-AIA or AIA Status*

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

*Allowable Subject Matter*

2. The following is an examiner's statement of reasons for allowance:

Claims 2-29 are allowable over the art of record.

The prior art taken alone or in combination failed to teach or suggest:

“detecting one or more payment accepting units in proximity to the mobile device, including detecting predefined radio transmissions broadcast by the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services, and displaying a user interface of a mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input to (i) receive selection by a user of the mobile device of an available payment accepting unit of the one or more payment accepting units and (ii) trigger payment by the mobile payment application for a transaction initiated by the user of the mobile device with the available payment accepting unit of the one or more payment accepting units” as recited in independent claims 2, 16 and 23.

The above recited limitations provide meaningful limitations that transforms the abstract idea into patent eligible. Each of the independent claims as a whole effects an improvement to

another technology or technical field. These limitations in combination provide meaningful limitations beyond generally linking the use of the abstract idea to a practical application.

Aument (US Patent No. 11182794 B1) discloses a payment reader and a POS terminal to communicate over a wireless connection. The methods and systems include monitoring one or more parameters corresponding to a payment reader and another device in proximity to the payment reader. The first device, through a set of customized instructions, determines whether behavior of the second device substantially corresponds to the first device, in order to detect suspected hardware or software intrusion associated with the secure first device. On successful detection of a suspected intrusion, the first device generates an alert for a user of the first device if illegal intrusion is suspected by the processor.

Silva et al (US 20160098690 A1) disclose a wireless-enabled kiosk system and associated method for recycling and performing other processes with mobile phones and other electronic devices are described herein. In various embodiments, the present technology includes systems and methods for wirelessly connecting a consumer-operated kiosk with an electronic device to facilitate processing (e.g., purchasing) the device. In some embodiments, the present technology includes using a wireless link to identify a device, evaluate a device, resolve device issues to enable purchase of the device, locate a device, etc. Various other aspects of the present technology are described herein.

*Conclusion*

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to FRANTZY POINVIL whose telephone number is (571)272-6797. The examiner can normally be reached M-Th 7:00AM to 5:30PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Anderson can be reached on 571-270-0508. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: <https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent-center> for more information about Patent Center and <https://www.uspto.gov/patents/docx> for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/fp/

/FRANTZY POINVIL/  
Primary Examiner, Art Unit 3698

September 20, 2022

<b>Notice of References Cited</b>	Application/Control No. 17/147,305	Applicant(s)/Patent Under Reexamination Patel, Paresh K.	
	Examiner FRANTZY POINVIL	Art Unit 3698	Page 1 of 1

**U.S. PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-11182794-B1	11-2021	Aument; Todd A.	G06Q20/3278	1/1
*	B	US-20200387881-A1	12-2020	Smith; Lincoln	G07C9/37	1/1
*	C	US-20180315271-A1	11-2018	Gharabegian; Armen Sevada	F03G6/001	1/1
*	D	US-20160098690-A1	04-2016	Silva; John	H04W4/80	705/21
*	E	US-9272713-B1	03-2016	Dvoskin; Daniel	B60K28/02	1/1
*	F	US-20130087050-A1	04-2013	Studor; Charles F.	A47J31/525	99/279
*	G	US-20070159994-A1	07-2007	Brown; David L.	H04W12/02	370/324
	H					
	I					
	J					
	K					
	L					
	M					

**FOREIGN PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

**NON-PATENT DOCUMENTS**

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Kumar, "Amazon gets Indian patent for auto authentication of mobile transactions", ProQuest document Id: 2433007646, Financial Express, 13 August (Year: 2020).
	V	
	W	
	X	

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.



UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

24341 7590 09/22/2022
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

Table with 2 columns: EXAMINER (HOLLY, JOHN H), ART UNIT (3696), PAPER NUMBER (6900)

DATE MAILED: 09/22/2022

Table with 5 columns: APPLICATION NO. (17/529,111), FILING DATE (11/17/2021), FIRST NAMED INVENTOR (PARESH K. PATEL), ATTORNEY DOCKET NO. (104402-5056-US), CONFIRMATION NO. (6900)

TITLE OF INVENTION: SYSTEMS AND METHODS FOR DETERMINING ELECTRIC PULSES TO PROVIDE TO AN UNATTENDED MACHINE
BASED ON REMOTELY-CONFIGURED OPTIONS

Table with 7 columns: APPLN. TYPE (nonprovisional), ENTITY STATUS (SMALL), ISSUE FEE DUE (\$600), PUBLICATION FEE DUE (\$0.00), PREV. PAID ISSUE FEE (\$0.00), TOTAL FEE(S) DUE (\$600), DATE DUE (12/22/2022)

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies. If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above. If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)". For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

**PART B - FEE(S) TRANSMITTAL**

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: **Mail Stop ISSUE FEE**  
**Commissioner for Patents**  
**P.O. Box 1450**  
**Alexandria, Virginia 22313-1450**

By fax, send to: **(571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the **ISSUE FEE** and **PUBLICATION FEE** (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

24341                      7590                      09/22/2022  
**Morgan, Lewis & Bockius LLP (PA)**  
**1400 Page Mill Road**  
**Palo Alto, CA 94304-1124**

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/529,111	11/17/2021	PARESH K. PATEL	104402-5056-US	6900

**TITLE OF INVENTION: SYSTEMS AND METHODS FOR DETERMINING ELECTRIC PULSES TO PROVIDE TO AN UNATTENDED MACHINE BASED ON REMOTELY-CONFIGURED OPTIONS**

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$600	\$0.00	\$0.00	\$600	12/22/2022

EXAMINER	ART UNIT	CLASS-SUBCLASS
HOLLY, JOHN H	3696	705-044000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.</p> <p><input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. <b>Use of a Customer Number is required.</b></p>	<p>2. For printing on the patent front page, list</p> <p>(1) The names of up to 3 registered patent attorneys or agents OR, alternatively, _____ 1</p> <p>(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. _____ 2</p> <p>_____ 3</p>
--	---

**3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)**

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE \_\_\_\_\_ (B) RESIDENCE: (CITY and STATE OR COUNTRY) \_\_\_\_\_

Please check the appropriate assignee category or categories (will not be printed on the patent) :  Individual  Corporation or other private group entity  Government

4a. Fees submitted:  Issue Fee  Publication Fee (if required)  Advance Order - # of Copies \_\_\_\_\_

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

Electronic Payment via EFS-Web  Enclosed check  Non-electronic payment by credit card (Attach form PTO-2038)

The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. \_\_\_\_\_

**5. Change in Entity Status** (from status indicated above)

Applicant certifying micro entity status. See 37 CFR 1.29

Applicant asserting small entity status. See 37 CFR 1.27

Applicant changing to regular undiscounted fee status.

**NOTE:** Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

**NOTE:** If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

**NOTE:** Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

**NOTE:** This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature \_\_\_\_\_ Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_ Registration No. \_\_\_\_\_

**Petitioner Exhibit 1002-4093**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes application details for PARESH K. PATEL and examiner HOLLY, JOHN H.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.



## OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

### Privacy Act Statement

**The Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

<b>Notice of Allowability</b>	<b>Application No.</b> 17/529,111	<b>Applicant(s)</b> PATEL, PARESH K.	
	<b>Examiner</b> JOHN H HOLLY	<b>Art Unit</b> 3696	<b>AIA (FITF) Status</b> Yes

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.  This communication is responsive to Amendment filed August 19, 2022.  
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on \_\_\_\_\_.
2.  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
3.  The allowed claim(s) is/are 2-31. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/pph/index.jsp](http://www.uspto.gov/patents/init_events/pph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).
4.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

**Certified copies:**

- a)  All      b)  Some\*      c)  None of the:
1.  Certified copies of the priority documents have been received.
  2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5.  CORRECTED DRAWINGS (as "replacement sheets") must be submitted.  
 including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
6.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |  |  |
|--|--|
| 1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 5. <input type="checkbox"/> Examiner's Amendment/Comment                             |
| 2. <input checked="" type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br>Paper No./Mail Date <u>August 19, 2022.</u> | 6. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| 3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material _____.                    | 7. <input type="checkbox"/> Other _____.   |
| 4. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date. _____.  |  |

/John H. Holly/  
Primary Examiner, Art Unit 3696

### **Notice of Pre-AIA or AIA Status**

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

### **DETAILED ACTION**

This communication is in response to an Amendments filed August 19, 2022.

### **Continued Examination Under 37 C.F.R. §1.114**

A request for continued examination ("RCE") under 37 C.F.R. §1.114, including the fee set forth in 37 C.F.R. §1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 C.F.R. §1.114, and the fee set forth in 37 C.F.R. §1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 19, 2022 has been entered.

### **. Information Disclosure Statement**

The Information Disclosure Statement (IDS) submitted on August 19, 2022 was filed in compliance with the provisions of 37 CFR 1.97. Accordingly, this Information Disclosure Statement is being considered by the Examiner.

### **Allowable Subject Matter**

Claims 2 – 31 are allowed over prior art of record.

## Reasons for Allowance

The following is an examiner's statement of reasons for allowance:

The prior art of record neither anticipates nor renders obvious the claimed subject matter of the instant application as a whole either taken alone or in combination, in particular, prior art of record does not teach “detecting a selection of a first user interface object that corresponds to a first option in the first set of remotely-configured options; after detecting the selection of the first user interface object, receiving, from the server, pulse information specifying a count, amplitude, shape, or interval of electric pulses to be provided to the control unit of the unattended machine by the pulse-providing device in accordance with the first option; in accordance with a determination that a trigger condition has been satisfied, sending the pulse information to the pulse-providing device; and at the pulse-providing device: receiving the pulse information; determining based on the received pulse information a signal sequence of electrical pulses to output to the control unit of the unattended machine in order to initiate a cashless operation of the unattended machine, wherein the signal sequence of electrical pulses emulates an analog signal generated by a coin receiving switch of the unattended machine, and wherein the signal sequence is characterized by the count, amplitude, shape, or interval of electric pulses specified by the pulse information; and causing the unattended machine to initiate the cashless operation by issuing the signal sequence of electrical pulses to the control unit.”.

The following prior art references have been deemed most relevant to the allowed claim(s):

The closest prior art Mordechai Teicher (Pub. # US 2010/0312692 A1) teaches a compact payment terminal for operating upon a purchase made by a customer at a retail device is provided. The customer carries a mobile communication device that includes a payment module and a communication module. The compact payment terminal includes a first interface for interfacing with the retail device, a second interface

for interfacing with the mobile communication device of the customer and a processing unit connected to the first and second interface. The compact payment terminal is configured to receive, via the first interface, a payment request from the retail device, cooperate, via the second interface, with the payment module of the mobile communication device for initiating a payment transaction respective to the payment request, and selectably conduct, via the second interface and the communication module of the mobile communication device, a communication session between the processing unit and at least one server.

The closest prior art Jonathan L. Lei et al. (Pub. # US 2003/0158891 A1) teaches a wireless network system includes a server system connected to a network. An electronic device is provided having a wireless transceiver adapted to communicate via at least one of light transmission and radio frequency (RF) transmission. A portable wireless device is provided having a wireless connection to the network. The portable wireless device is adapted to communicate wirelessly with the electronic device. The electronic device communicates with the server system over the network through the portable wireless device. The electronic device may conduct real-time and/or non-real-time transactions with the server system by utilizing the portable wireless device as a communication proxy.

.  
.

The arguments presented by the Applicant along with the combination of elements, such as, "determining based on the received pulse information a signal sequence of electrical pulses to output to the control unit of the unattended machine in order to initiate a cashless operation of the unattended machine, wherein the signal sequence of electrical pulses emulates an analog signal generated by a coin receiving switch of the unattended machine, and wherein the signal sequence is characterized by the count, amplitude, shape, or interval of electric pulses specified by the pulse information.". The claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks and recite significantly more than an abstract idea.

### **Conclusion**

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

### **Contact Information**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John H. Holly whose telephone number is 571.270.3461. The examiner can normally be reached on MON. - FRI 10 AM - 8 PM p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Namrata Boveja can be reached on (571)-272-8105. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/John H. Holly/

Primary Examiner, Art Unit 3696

**Notice of References Cited**

Application/Control No. 17/529,111	Applicant(s)/Patent Under Reexamination PATEL, PARESH K.	
Examiner JOHN H HOLLY	Art Unit 3696	Page 1 of 1

**U.S. PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20100312692-A1	12-2010	TEICHER; MORDECHAI	G06Q20/3278	455/414.1
*	B	US-20030158891-A1	08-2003	Lei, Jonathan L.	G06Q20/327	709/203
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

**FOREIGN PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

**NON-PATENT DOCUMENTS**

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
*	U	ProQuestDialogNPL Search History
	V	
	W	
	X	

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
 Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.



Espacenet

**Bibliographic data: KR20130138637 (A) — 2013-12-19**


---

**PERSONAL MARKETING SYSTEM AND METHOD USING MOBILE COUPON AND ONLINE SHOPPING**

**Inventor(s):** AHN DAE HYOUNG [KR]; JANG HYEON JU [KR] ± (AHN, DAE HYOUNG, ; JANG, HYEON JU)

**Applicant(s):** LEEAHNDIGITAL CO LTD [KR] ± (LEEAHNDIGITAL CO., LTD)

**Classification:** - **international:** G06Q30/02  
 - **cooperative:** G06Q30/0208 (KR); G06Q30/0233 (KR)

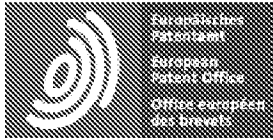
**Application number:** KR20120099066 20120907 Global Dossier

**Priority number(s):** KR20120061872 20120611

**Abstract of KR20130138637 (A)**

The present invention relates to a personal marketing system using a mobile coupon and online shopping and a method thereof. The personal marketing system according to the present invention includes a coupon service providing server, a coupon issuing member terminal, and a coupon receiving member terminal. [Reference numerals] (AA) Coupon issuing member terminal;(BB) Coupon service providing server;(CC) Coupon receiving member terminal;(S110) Transmit an authenticcode;(S120) Authentication;(S130) Authentication approval;(S140) Set a receiver;(S145) Set a target;(S150) Set a reward;(S157) Temporary payment;(S160) Request to issue a coupon;(S170,S240) Verification;(S180) Approve coupon issuing;(S190) Store coupon-related information;(S200) Issue the coupon;(S210) Transmit the coupon-related information;(S220) Perform a target;(S230) Request the reward;(S235) Payment;(S250) Receive compensation;(S260) Not perform the target;(S267) Refunds





# Patent Translate

Powered by EPO and Google

## Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

## DESCRIPTION KR20130138637A

<sup>11</sup> Personal marketing system and method using mobile coupon and online shopping  
{Personal marketing system and method using mobile coupon and online shopping}

### [0001]

<sup>16</sup> The present invention relates to a personal marketing system and method for managing individual customers by using mobile accumulation coupons (points, points, stamps, etc.) and online shopping. More specifically, the present invention provides a function of providing a mobile coupon to a mobile communication terminal of a customer who is registered as a member of a coupon service provider, and by utilizing this function, the member provides a mobile accumulated coupon and reward to other members using the service. , compensation), the service user issues a mobile accumulation coupon through the provided function, issues it, and designates a corresponding reward (online product or product exchange voucher) in an online shopping mall when a specific target number is reached at the same time , A personal marketing system and method using a mobile accumulation coupon and online shopping in which, when a user who receives a coupon reaches a certain number through a specific activity, the corresponding accumulation coupon is automatically changed to a pre-specified reward.

### [0002]

<sup>33</sup> Nowadays, in the era of personal brands, one-person companies and personal brands are emerging, and marketing is no longer limited to companies and stores. As people communicate through SNS and smartphones, individual name values, social positions, relationships, and personal connections are becoming more and more important.

[0003]

40 In particular, the use of mobile coupons has increased in proportion to the rapid spread of mobile terminals, and culturally, they are becoming established as a form of payment method that is easy to carry and convenient to use.

[0004]

46 In the past, in existing marketing that required a lot of infrastructure, marketing by one- person companies and individuals was difficult, but now, marketing by one- person companies and individuals has become easier through mobile apps, and in particular, the emergence of various services through mobile apps Using mobile advertisements and coupons, easier and more effective marketing activities have become possible.

52 Accordingly, a simpler and more convenient personal marketing method using a smartphone has been demanded.

[0005]

57 Accordingly, the present invention proposes a personal marketing system and method for managing individual customers using mobile coupons (points, points, stamps, etc.) and online shopping.

[0006]

63 The present invention provides a function of providing a mobile coupon to a mobile communication terminal of a customer who has registered as a member of a coupon service provider, and by utilizing this function, a member provides a mobile accumulation coupon and a reward to other members using the corresponding service.

67 In the present invention, the service user issues a mobile accumulation coupon through the provided function, issues it, and at the same time, when a specific target number is reached, a corresponding reward (online product or product voucher) is designated within the designated online shopping mall or service, and the coupon is redeemed. The provided user reaches a specific number through specific activities, and the corresponding accumulation coupon is automatically changed to a pre- specified reward.

[ ]

77 The problem to be solved by the present invention is to provide a function of providing a mobile coupon to a mobile communication terminal of a customer who is registered as a member of a coupon service provider, and by utilizing this function, a

member can redeem a mobile accumulated coupon and reward to other members who use the service. To provide a personal marketing system and method for managing individual customers using mobile coupons (points, points, stamps, etc.) and online shopping, which provide

84 Another problem to be solved by the present invention is that the service user issues a mobile accumulation coupon through the provided function, and at the same time, when a specific target number is reached, a corresponding reward (online product or product exchange voucher) is provided to an online shopping mall or service. When a user who receives a coupon reaches a certain number through a specific activity, the coupon is automatically changed to a pre-specified reward. To provide a personal marketing system and method for managing individual customers using shopping.

91 In order to solve the above problems, in the personal marketing method using a mobile accumulated coupon and online shopping according to the first embodiment of the present invention, a coupon issuing member terminal installed by receiving a service program provided by a coupon service provider, coupons a receipt condition storage step of temporarily storing coupon recipient information including recipient member terminal information and target information for receiving a reward; After the receipt condition storage step, the coupon issuing member terminal temporarily stores the set reward, the reward storage step; After the reward storage step, a payment step of making a payment for the set reward in the coupon issuing member terminal; After the payment step, the coupon issuing member terminal transmits the issued coupon to the coupon receiving member terminal, and at the same time, the set goal and reward information is also transmitted to the coupon receiving member terminal; One of the coupon service provider server or coupon issuing member terminal receives the target performance result from the coupon receiving member terminal and, when it is determined that the target performance is complete, provides a reward (compensation) to the coupon receiving member terminal; a reward receiving step; It is characterized by comprising.

108 In the personal marketing method using a mobile accumulated coupon and online shopping according to a second embodiment of the present invention, a coupon issuing member terminal installed by receiving a service program provided by a coupon service provider includes coupon receiving member terminal information a receipt condition storage step of temporarily storing coupon recipient information and target information for receiving a reward (compensation); After the receipt condition storage step, the coupon issuing member terminal temporarily stores the set reward, the reward storage step; After the reward storage step, a temporary payment step of making a temporary payment for the set reward in the coupon issuing member terminal; After the provisional payment step, the coupon issuing member terminal transmits the issued coupon to the coupon receiving member terminal, and at the same time, the set goal and reward information is also transmitted to the coupon receiving member terminal; After the coupon receiving step, if one of the coupon service provider server or the coupon issuing member

terminal receives the target performance result from the coupon receiving member terminal and determines that the target performance is complete, in the provisional payment step, automatically pays the paid reward and providing a reward (compensation) to the coupon receiving member terminal; after the coupon receiving step, either the coupon service provider server or the coupon issuing member terminal receives the target performance result from the coupon receiving member terminal, If it is determined that the target performance has not been completed, in the temporary payment step, a reward refund step of refunding the paid reward.

- 130 Prior to the receiving condition storage step, the coupon issuing member terminal transmits one or more of the authentication code or ID and password or personal barcodes previously issued by the coupon issuing member to the coupon service provider server to perform authentication. ; more includes
- 134 Rewards are online products, coupons, gift certificates, or stamps. In particular, rewards are online products, coupons, or gift certificates of online shopping malls of member companies affiliated with coupon service providers, or online shopping malls of member companies affiliated with coupon service providers. or a stamp.
- 138 In the coupon receiving step, the issued coupon requesting issuance of the coupon from the coupon issuing member terminal to the coupon service provider server; The coupon service provider server verifies whether or not the requested coupon is issued, transmits a coupon issuance approval signal to the coupon issuing member terminal, and stores coupon- related information; The coupon issuance member terminal issuing a coupon;
- 144 In the coupon receiving step, the issued coupon may be a cumulative coupon including points and stamps.
- 146 In the first embodiment, in the reward receiving step, if one of the coupon service provider server or coupon issuing member terminal receives a target performance result from the coupon receiving member terminal, but determines that the target performance is not completed, the payment step It further includes a reward refund step in which the reward paid in is refunded.
- 151 In the present invention, the coupon issuing member terminal may be a parent's terminal, and the coupon receiving member terminal may be a child's terminal.
- 153 In the present invention, the coupon issuing member terminal is a terminal of a single entrepreneur, and the coupon receiving member terminal may be a terminal of a customer of the single entrepreneur.
- 156 In the present invention, the coupon issuing member terminal may be the same as the coupon receiving member terminal.
- 158 In addition, the personal marketing system using mobile accumulated coupons and online shopping of the present invention provides a service program (app program) for issuing mobile coupons to members, and coupons for managing coupons and rewards (compensation) issued by members service provider servers; Using the service program, a coupon issuing member terminal in which coupon recipients, receipt conditions, rewards (compensation) are set, and mobile accumulation

coupons are issued; and a coupon receiving member terminal which receives coupons, receipt condition information, and reward information from the coupon issuing member terminal, and receives a reward (compensation) when the goal included in the receipt condition information is completed.

- 168 The coupon issuing member terminal is configured to make a payment for the set reward, and one of the coupon service provider server or coupon issuing member terminal receives the target performance result from the coupon receiving member terminal, but determines that the target performance is not completed. In this case, the reward paid in the payment step is automatically refunded.
- 173 The coupon issuing member terminal is configured to make a provisional payment when a reward is set.
- 175 One of the coupon service provider server or coupon issuing member terminal receives the target performance result from the coupon receiving member terminal and when it is determined that the target performance is complete, the coupon issuing member terminal automatically pays for the paid reward, and rewards (compensation ) is provided to the coupon receiving member terminal.
- 180 If one of the coupon service provider server or the coupon issuing member terminal receives the target performance result from the coupon receiving member terminal, but determines that the target performance is not completed, the coupon issuing member terminal refunds the paid reward.
- 184 According to the personal marketing system and method for managing individual customers using mobile accumulation coupons (points, points, stamps, etc.) and online shopping of the present invention, mobile coupons are provided to mobile communication terminals of customers who are registered as members of coupon service providers. It provides a function to provide, and by utilizing this, members provide mobile accumulation coupons and rewards to other members who use the service.
- 191 In addition, in the present invention, the service user issues a mobile accumulation coupon through the provided function, and at the same time as issuing it, when a specific target number is reached, a corresponding reward (online product or product exchange voucher) is designated in the online shopping mall, and the coupon When a user who has been provided with a certain number reaches a certain number through a specific activity, the corresponding accumulation coupon is automatically changed to a pre- specified reward.
- 198 The present invention can be used for educational purposes in one- person companies and relationships between parents and children.
- 200 For example, a parent may present a predetermined target value as a reward while issuing a mobile coupon to a child, and the child may receive a reward by achieving the predetermined target value.
- 203 As another example, a single entrepreneur can issue coupons to his or her customers and use them for customer marketing.

[0029]

- 208 1 is an explanatory diagram schematically illustrating a personal marketing system using a mobile accumulated coupon and online shopping according to an embodiment of the present invention.
- 211 2 is an explanatory diagram for briefly explaining the structure of a service in a personal marketing method using a mobile accumulated coupon and online shopping according to an embodiment of the present invention.
- 214 Figure 3 is a flowchart schematically illustrating a personal marketing method using a mobile accumulated coupon and online shopping according to an embodiment of the present invention.
- 217 Figure 4 is a flowchart schematically illustrating a personal marketing method using a mobile accumulated coupon and online shopping according to another embodiment of the present invention.
- 220 5 is a flowchart schematically illustrating a personal marketing method using a mobile accumulated coupon and online shopping according to another embodiment of the present invention.
- 223 6 is a flowchart for explaining reward payment and delivery according to an embodiment of the present invention.
- 225 7 is a flowchart for explaining reward payment and delivery according to another embodiment of the present invention.
- 227 8 is an explanatory diagram illustrating a case of issuing a coupon through a coupon issuing member terminal in the present invention.
- 229 9 is an explanatory diagram illustrating a case of issuing a coupon in a recipient terminal in the present invention.
- 231 10 is a flowchart of an embodiment of an issuer authentication method when directly issuing a coupon from a recipient terminal in the present invention.
- 233 11 is a flowchart of another embodiment of an issuer authentication method when directly issuing a coupon from a recipient terminal in the present invention.
- 235 11 is an issuer authentication method through a mobile authenticator.
- 236 12 is an example of issuing a coupon using a recipient terminal in the personal marketing system of the present invention.
- 238 13 is another example of issuing a coupon using a recipient terminal in the personal marketing system of the present invention.
- 240 14 is an example of screens showing coupon creation and reward reception in the personal marketing system of the present invention.

[0030]

245 Hereinafter, a personal marketing system and method using a mobile accumulated coupon and online shopping according to the present invention will be described in detail with reference to the accompanying drawings.

[0031]

257 1 is an explanatory diagram schematically illustrating a personal marketing system using a mobile accumulated coupon and online shopping according to an embodiment of the present invention.

[0032]

257 The coupon service provider server 100 provides a service program (app program) having a function of providing mobile coupons to the mobile communication terminals of members registered through authentication, that is, the member terminals 210 and 250, Coupons issued by the member terminals 210 and 250 are managed.

[0033]

264 The member terminal 210 provides mobile accumulation coupons and rewards to other member terminals 250 using the service program.

266 The member issues a mobile accumulation coupon through the provided function of the service program in the member terminal 210, and at the same time designates a corresponding reward provided when a specific target number is reached in the online shopping mall.

270 The reward may be an online product or a product voucher.

[0034]

274 When a certain number is reached through a specific activity in another member terminal 250 provided with a coupon, the corresponding accumulation coupon is automatically changed to a previously designated reward.

277 Here, whether or not a specific target value is reached may be checked through the coupon service provider server.

[0035]

282 The service in the personal marketing system of the present invention is a method of directly selecting a reward for a accumulated coupon by linking it with online shopping by issuing a coupon through a mobile device.

285 When a user reaches a certain target value, the coupon is automatically changed into a gift certificate that can be exchanged for a reward product or product set by the coupon issuer in advance.

[0036]

<sup>291</sup> Here, the terms used in the present invention are explained as follows.

[0037]

<sup>295</sup> Issuance of a coupon refers to the creation of a coupon of the corresponding issuer in the terminal of the coupon recipient through the input of a specific authentication code or the issuer's related information. When the coupon is issued, the coupon information (ie coupon issuance date, expiration date, type of coupon (stamp or point, etc.), goal (mission) and reward, and member information (phone number, name or ID or terminal identification code) are delivered.

<sup>301</sup> In particular, in the present invention, coupons are basically issued directly by members to other members, but approval from coupon service providers may be required for certain rules such as coupon rules.

[0038]

<sup>307</sup> The target number is reaching a certain number, and may be, for example, the number of stamps, the number of points, the number of store visits, or the number of meetings with the issuer.

[0039]

<sup>313</sup> In the present invention, the number of issued coupons and the number of rewards must always match.

[0040]

<sup>318</sup> Reward setting refers to selecting a related product or online product from a shopping mall built directly within the service by the corresponding coupon service company or from another service vendor (easily explained, an online shopping mall) of the affiliated company and making payment.

[0041]

<sup>325</sup> In general, there are two ways to set up rewards.

[0042]

<sup>329</sup> The first is a case in which the issuer designates coupon rules in advance, but sets (purchases) a reward when designating coupon rules. Coupons are subsequently issued and used according to preset coupon rules within the set rewards.

Petitioner Exhibit 1002-4110



332 In this case, the equation of issuer = coupon rule holds, and if the rewards of coupons issued by the issuer are all the same, the number of rewards and the number of coupons that can be issued are the same (the number of rewards = the number of coupons that can be issued).

336 For example, if 5 rewards are purchased, the issuer can only issue 5 coupons.

#### [0043]

340 Second, in the case where the issuer designates coupon rules for each coupon issuance, the issuer must pay the reward each time the coupon is issued.

342 In this case, the equation of recipient = coupon rule holds, and the issuer can make a different coupon each time it issues a coupon after selecting a recipient on the coupon recipient terminal or online (remote issuance). Each time it is issued, coupon rules are created, and in this case, rewards can be designated differently for each recipient.

#### [0044]

350 In addition, if the reward remains after paying or refunding the reward in advance, the reward can be set in the reward list without separate payment.

#### [0045]

355 The set goal performance is regarded as goal performance when the recipient of the coupon reaches the goal within the period set by the issuer (for example, if the goal is to stamp 10 stamps, stamping all 10 stamps is called goal performance).

#### [0046]

361 Non-performance of the set goal is regarded as non-performance if the target is not reached within the specified period or if the target is reached but the period has elapsed, and even if the recipient deletes the coupon or deletes the service program.

#### [0047]

367 In the present invention, the performance of the target can be judged by two things.

#### [0048]

371 The first is numerical comparison, in which the server compares the recipient's numerical value and the number of target values over a certain period of time and checks the validity period to determine the mission performance.

[0049]

377 Second, if the target completes the numerical value within the specified period, a button such as 'Get Reward' or 'Mission Complete' is activated or created on the recipient's coupon (through the server check process of the first numerical comparison), and the recipient clicks this button. If so, the server checks the relevant information and if there is no abnormality, the mission is deemed completed and a reward is provided (the corresponding coupon is deleted and replaced with a reward).

[0050]

387 Thirdly, regardless of the number (the server does not check it separately), when the 'Mission Complete' or 'Get Reward' button is put in the coupon and the button is clicked, the server proceeds with the first numerical comparison process, and when the information is matched, the mission In case of completion or information inconsistency, it is confirmed as mission failure.

[0051]

395 In the present invention, the role of the coupon service provider server can be largely referred to as information transmission and reception, and information generation.

398 Information transmission and reception here is, firstly, interlocking coupon information of the issuer and recipient of the coupon, secondly, transmission and execution of rules defined in advance when coupon rules are created in advance, and thirdly, transmission and reception of authentication information of the issuer and determining whether or not they match.

403 The generation of information here refers to the creation and linkage of coupon information between the issuer and the receiver.

[0052]

408 2 is an explanatory diagram for briefly explaining the structure of a service in a personal marketing method using a mobile accumulated coupon and online shopping according to an embodiment of the present invention.

[0053]

414 As an execution step, this service program is installed and executed (S10).

415 Execution of the service of the present invention includes all mobile devices capable

of executing apps, including smart phones, and online.

[0054]

420 As a sign- up step, member sign- up is performed through the installed service program (S20).

[0055]

425 As a recipient selection step, a member who wishes to issue a coupon sets a recipient to receive the coupon in the coupon issuing member terminal (S140).

427 In selecting the recipient of the coupon, the recipient can be selected from the terminal (device) of the member issuing the coupon, and in some cases, the coupon can be directly issued from the terminal of the recipient.

430 When issued directly from the recipient's terminal, a separate recipient selection step is not required.

[0056]

435 As a condition input step, a target of a specific activity is set in the coupon issuing member terminal (S145).

437 That is, the coupon information (rule) is transmitted from the coupon issuing member terminal to the coupon service provider server, and the coupon service provider server receives it.

[0057]

443 In the reward selection step, a reward is set in the coupon issuing member terminal (S150).

445 Accordingly, the coupon service provider server makes a payment request to the coupon issuing member terminal for the set reward.

[0058]

450 As a payment step, payment for the set reward is performed (S155).

451 That is, the member purchases a reward by transmitting payment information through the coupon issuing member terminal, and the coupon service provider server confirms the payment.

[0059]

457 In the coupon issuance step, the coupon issuing member terminal 210 issues a  
Petitioner Exhibit 1002-4113

coupon either through the coupon service provider server 100 or directly (S200).  
459 It is issued directly from the terminal 250 of the recipient.

[0060]

463 Here, when a member requests a coupon service provider server to issue a coupon and the coupon service provider server issues a coupon to another member, the member (issuer) inputs the coupon rules (i.e., the contents of the coupon) to the coupon service provider server (website or program), and the coupon service provider server reviews and approves the contents.

468 In addition, when a member directly issues a coupon to another member, there may be two methods.

470 One is when a coupon is issued remotely by searching for a member online (website or program). This is the case of issuing the creation.

[0061]

475 In the coupon receiving step, the issued coupon is transmitted from the coupon service provider server 100 or the coupon issuing member terminal to the coupon receiving member terminal (S210).

[0062]

481 In the target performance step, the coupon receiving member who has received the coupon performs the target performance through the coupon receiving member terminal (S220).

[0063]

487 In the reward receiving step, when the target performance is completed in the target performing step, a reward (compensation) is provided to the coupon receiving member terminal (S250), and consequently, the coupon is changed to a reward.

490 That is, when the coupon service provider server determines that the final performance target value of another member and the issuer's set target value are the same for the related target value (in principle, the coupon service provider server confirms), the reward is transmitted.

[0064]

497 In the present invention, rewards are provided to other members by a coupon service provider.

499 When a reward is purchased, the coupon service company holds the reward

temporarily and delivers it when the goal is fulfilled.

[0065]

*504* Figure 3 is a flow chart schematically illustrating a personal marketing method using a mobile accumulated coupon and online shopping according to an embodiment of the present invention.

[0066]

*510* The member 210 subscribes to the mobile coupon issuance service, and stores the service program provided by the mobile coupon issuance service in the user's terminal.

[0067]

*516* In the authentication step, the member 210 who has subscribed to the mobile coupon issuance service provides the coupon service by using the authentication code or ID and password or personal barcode issued in advance through the coupon issuing member terminal, which is his or her online or mobile terminal. Authentication is requested while transmitting to the provider server 100 (S110), the coupon service provider server 100 performs authentication (S120), and transmits an approval signal to the coupon issuing member terminal (S130).

[0068]

*526* As a recipient setting step, a recipient is set in the coupon issuing member terminal to issue a coupon (S140).

[0069]

*537* As a condition input step, a target of a specific activity is set in the coupon issuing member terminal (S145).

[0070]

*536* As a reward setting step, the coupon issuing member terminal sets a reward (S150).

[0071]

*540* As a payment step, payment for the set reward is performed (S155).

[0072]

*544* In the coupon issuance step, the coupon issuing member terminal requests coupon issuance to the coupon service provider server 100 (S160), and the coupon service provider server 100 verifies whether or not the coupon issuance requested by the coupon issuing member terminal. (S170), transmits a coupon issuance approval signal (S180), stores coupon- related information (S190), and issues a coupon (S200).

[0073]

*553* In some cases, the coupon service provider server 100 requests coupon issuance (S160), and the coupon service provider server 100 verifies whether or not the coupon is issued requested by the coupon issuing member terminal (S170), and issues the coupon. The transmission of the approval signal of (S180) may be omitted, and the coupon may be issued directly from the coupon issuing member terminal.

[0074]

*562* In the coupon receiving step, the issued coupon is transmitted from the coupon service provider server 100 or the coupon issuing member terminal to the coupon receiving member terminal, and at the same time, coupon- related information is also transmitted (S210).

*566* The coupons issued here may be accumulation- type coupons such as points or stamps.

[0075]

*571* In the target performance step, the coupon receiving member who has received the coupon and coupon- related information performs the target performance through the coupon receiving member terminal (S220).

[0076]

*577* In the reward receiving step, a reward request is made to the coupon service provider server 100 (S230), the coupon service provider server 100 verifies the reward request received from the coupon receiving member terminal (S240), and rewards the coupon It is provided to the receiving member terminal (S250).

[0077]

584 In some cases, a request for a reward is made to the coupon service provider server 100 (S230), and the coupon service provider server 100 omits the verification of the reward request received from the coupon receiving member terminal (S240), and the coupon The issuing member terminal or the coupon service provider server 100 may directly provide rewards to the coupon receiving member terminal.

#### [0078]

592 In FIG. 3, the payment for the reward set in the payment step is unconditionally carried out (S155), and if the coupon receiving member does not complete the goal through the coupon receiving member terminal, no refund is made.

595 Rewards will be refunded to the member issuing the coupon as it was purchased.

596 In this case, the purchased reward must be exhausted, and there is no refund.

#### [0079]

600 Figure 4 is a flowchart schematically illustrating a personal marketing method using a mobile accumulated coupon and online shopping according to another embodiment of the present invention.

#### [0080]

606 Instead of the payment step of FIG. 3, FIG. 4 has a provisional payment step, that is, in the provisional payment step of FIG. 4, a provisional payment is made for the set reward (S157).

#### [0081]

612 In addition, in FIG. 4, prior to providing the reward to the coupon receiving member terminal (S250) during the reward receiving step, there is a payment step of automatically paying for the set reward (S157).

#### [0082]

618 If the coupon receiving member who has received the coupon and coupon-related information fails to complete the goal through the coupon receiving member terminal (S260), the provisional payment for the set reward (S157) is automatically refunded (S267), and the refund Certain fees may apply.

622 Other than this, the personal marketing method of FIG. 4 is the same as the personal marketing method of FIG. 3 .

[0083]

627 5 is a flowchart schematically illustrating a personal marketing method using a mobile accumulated coupon and online shopping according to another embodiment of the present invention.

[0084]

633 In FIG. 5 , when the coupon receiving member who has received the coupon and coupon- related information fails to complete the goal through the coupon receiving member terminal (S260), the set reward (S155) is automatically refunded (S267).

636 Other than this, the personal marketing method of FIG. 5 is the same as the personal marketing method of FIG. 3 .

638 In case of refund, certain fees may be incurred.

[0085]

642 That is, in the case of FIG. 3, when payment is made for the set reward (S155), the purchased reward is not refundable regardless of whether the coupon receiving member performs the goal, whereas in the case of FIG. 5, after the set reward is paid (S155) S155), the purchased reward is refunded when the coupon receiving member fails to fulfill the goal (S267).

[0086]

650 In other words, the service of the present invention is a method of issuing a coupon through a mobile device and directly selecting a reward for an accumulation coupon by linking it with online shopping. is changed to a gift certificate that can be exchanged for a reward product or product specified by the coupon issuer, which is summarized as follows.

[0087]

658 First, to summarize the mobile coupon issuance service, the user who has subscribed to the mobile coupon issuance service issues a mobile coupon to a third party through an authentication code or ID and password or personal barcode issued in advance through online and mobile devices this is possible

662 The coupon to be issued is an accumulation type coupon such as a point or a stamp. When the coupon is issued, a certain target value is set, and when the target value of the corresponding coupon is reached, the reward provided is designated by selecting a product or gift certificate from a shopping mall provided by the service or a related shopping mall.

667 The designated product or gift certificate is automatically changed or purchased

Petitioner Exhibit 1002-4118



when the user who has been issued the coupon completes the target.

669 (Mission Complete)

[0088]

673 Second, to summarize the reward (reward), in the present invention, the reward (reward) in the corresponding service includes real or online products, coupons, gift certificates, stamps, etc. that require payment.

676 The user issuing the coupon must pay for the reward product at the issuance stage when the coupon is issued.

678 Payment is not necessarily an act of paying an amount, but includes a payment step.

679 The online product referred to here refers to the real thing that can be used online, and gift certificates include coupons or gift certificates that can be used in online services, or gift certificates that can be exchanged for goods that can be used for offline payment.

683 Coupons in compensation refer to various discount coupons and event coupons.

684 A stamp in compensation literally means a stamp.

[0089]

688 For example, a person named A, while issuing a coupon named A' , purchases and selects 4 stamps of a popular cafe named B in Hongik University as a coupon reward.

[0090]

694 When user C receives coupon A' and completes the target, if user C holds stamp coupon B' of cafe B within the service, 4 stamps are added from stamp coupon B' , and stamp coupon B If you don't have one, you will receive a stamp coupon B with 4 stamps.

698 In the case of this user, if he is supposed to receive a cup of Americano as a reward when he stamps all 8 stamp coupons B', he can drink Americano by stamping 4 more stamps.

701 Stamp coupon B is a mobile stamp coupon provided by cafe B, and the coupon may be a coupon provided within the service or provided by another mobile coupon service, and in the latter case, the service is linked.

[0091]

707 Payment in the present invention may have three cases.

708 After payment, if the user completes the target within the period, the payment is made and if the target is not completed, it is refunded. Certain fees may apply.

Petitioner Exhibit 1002-4119

710 The other one is when the payment is unconditional and non-refundable, and the purchased reward must be exhausted.

712 There may be no refund action.

#### [0092]

716 Here, if payment is made unconditionally and refund is not made, if the purchased reward remains with the member who purchased the reward, the member can check related information on his or her device (coupon issuing member terminal) or on the web. You can also log in and check your personal information online, such as on the site, and the remaining rewards can be used when issuing other coupons.

721 In other words, if there is a reward, a list of available rewards is displayed at the payment stage and a selection can be made.

#### [0093]

726 Third, if the receipt of mobile coupons is summarized, coupons can be issued from users who use the service after subscribing to the corresponding service for receiving mobile coupons.

729 When the user who receives the coupon reaches the target value within the period suggested by the coupon, the corresponding accumulation coupon can automatically receive a predetermined online gift certificate, point, or physical reward.

732 To put it more simply, the accumulated coupon is automatically changed to a reward.

#### [0094]

736 Fourth, if the service utilization using the present invention is explained, the service can be used for educational purposes in the relationship between a single-person company and parents and children.

#### [0095]

742 For example, a parent with a child in the first grade of elementary school issues a mobile stamp coupon for the child's education.

744 The coupon is valid for one month, and if you run errands 10 times within that period, you will receive a 5,000 won online cultural gift certificate.

746 When the child runs 10 errands, the mobile coupon is automatically changed to an online cultural gift certificate.

#### [0096]

751 As another example, Mr. A, an insurance solicitor, issues coupons to 100 customers

he manages due to the nature of his work in which he has to meet and treat many customers.

754 Set a rule of 1 stamp for each meeting and 5 stamps for customer recommendation, and when 10 stamps are filled, XX Coffee Shop Americano Gift Corn is sent to that customer.

[0097]

760 In addition, in the present invention, it is possible to utilize the service utilization stamp as a new marketing method as a reward.

762 For example, cafe A provides stamps from their stamp coupons to insurance solicitor C, B, at a low price, so cafe A can expand its customer base and insurance solicitor C can do personal marketing at low cost. .

[0098]

768 Fifth, when explaining the structure of the service, execution of the service of the present invention includes all mobile devices capable of executing apps, including smart phones, and online.

[0099]

774 Members must sign up through the service program, and sign- up is done in a simple sign- up step.

[0100]

779 In selecting the recipient of the coupon, the recipient can be selected from the terminal (device) of the member issuing the coupon, and in some cases, the coupon can be directly issued from the terminal of the recipient.

782 When issued directly from the recipient's terminal, a separate recipient selection step is not required.

784 Also available online.

[0101]

788 In selecting a reward, the reward is set by shopping for a product in a shopping mall affiliated with or belonging to the corresponding service, just like shopping in an online shopping mall.

791 That is, the selection of a reward is possible with a plurality of products fixed in the service program, or a product can be selected from an actual online shopping mall.

793 When selecting a product from an existing online shopping mall, it proceeds through

linkage with the corresponding service.

[0102]

*798* Here, the shopping mall linked to or belonging to the service means a shopping mall within the service, in which a coupon provider creates a shopping mall on its own and provides a service within the service or within a program (direct service), and an existing online shopping mall. Including linked shopping malls, which is a case of consignment service by interlocking in a service or program.

[0103]

*806* 6 is a flowchart for explaining reward payment and delivery according to an embodiment of the present invention.

*808* 6 is a case in which a coupon provider itself provides a reward.

[0104]

*812* In the reward setting step, the issuer sets the reward through an online shopping mall or the like in the coupon issuing member terminal (S150).

[0105]

*817* In the payment request step, the coupon issuing member terminal sends a payment request along with transmission of payment information to the coupon service provider, that is, the coupon service provider server (S151- 1), and the coupon service provider receives the coupon from the coupon issuing member terminal. The received payment information is transmitted to the payment agency, that is, the payment agency server, and a payment request is made to the payment agency server (S151- 2).

[0106]

*827* In the approval step, the payment agency server makes a payment approval request to the coupon issuing member terminal of the issuer (S152- 1), the issuer approves through the coupon issuing member terminal, and the approval result is sent to the payment agency server. is transmitted (S152- 2).

[0107]

*834* In the payment step, after being approved in the approval step, the payment agency server makes a payment and completes the payment (S154), and the payment

agency server transmits payment information (ie, paid information) to the coupon service provider server, (S156- 1), the coupon service provider server transmits the received payment information to the coupon issuing member terminal of the issuer to confirm the payment information (S156- 2).

[0108]

*843* In the payment step, the payment agency pays the price to the coupon service provider (S157- 1), and the coupon service provider receives the payment from the payment agency (S157- 2).

[0109]

*849* The following describes the flow of providing a reward (ie, product/gift certificate) according to goal performance after a coupon is issued by the coupon service provider server and transmitted to the recipient.

[0110]

*855* In the target performance step, the coupon receiving member who has received the coupon performs the target performance through the coupon receiving member terminal (S220).

[0111]

*861* In the information receiving step, when the receiver completes the goal performance in the goal performance step, information indicating that the goal has been completed is transmitted to the coupon service provider server through the coupon receiving member terminal (S232).

[0112]

*868* In the reward receiving step, the coupon service provider server delivers a reward (compensation) composed of product/gift certificate to the recipient (S247), and the recipient receives the reward (compensation) composed of product/gift certificate (S250).

[0113]

*875* 7 is a flowchart for explaining reward payment and delivery according to another embodiment of the present invention.

*877* 7 is a case in which a reward is provided by an external shopping company.

[0114]

887 Reward setting step (S150) to payment step (S154, S156- 1, S156- 2) of FIG. 7 are the same as those of FIG.

883 Therefore, the description thereof is omitted.

[0115]

887 The payment step after the payment step (S154, S156- 1, S156- 2) is as follows.

[0116]

891 In the payment step, the payment agency pays the coupon service provider or (external) shopping company (S157- 1), and the coupon service provider or (external) shopping company receives the payment from the payment agency (S157- 1). S157- 2).

[0117]

898 The following describes the flow of providing rewards (ie, exchange vouchers/products) according to goal performance after coupons are issued by the coupon service provider server and transmitted to the recipients.

[0118]

904 In the step of delivering the product exchange voucher to the coupon service provider, the (external) shopping company delivers the product exchange voucher that can be exchanged for a reward product to the coupon service provider (S212), and the coupon service provider receives the product exchange voucher (S212). S214).

[0119]

912 In the target performance step, the coupon receiving member (receiver) who has received the coupon performs the target performance through the coupon receiving member terminal (S220).

[0120]

918 In the information receiving step, when the receiver completes the goal performance in the goal performance step, information indicating that the goal has been completed

is transmitted to the coupon service provider server through the coupon receiving member terminal (S232).

[0121]

<sup>925</sup> In the step of delivering the product exchange voucher to the coupon receiving member, the coupon service provider server delivers the product exchange voucher to the coupon receiving member (receiver) (S243), and the coupon receiving member (receiver) receives the product exchange voucher (S244).

[0122]

<sup>932</sup> The coupon receiving member is in the product receiving stage, and the coupon receiving member (recipient) exchanges or applies for the product (S246), and accordingly, the (external) shopping company delivers the product (S247), resulting in the coupon receiving member (recipient) receives the goods

[0123]

<sup>939</sup> 8 is an explanatory diagram illustrating a case of issuing a coupon through a coupon issuing member terminal in the present invention.

[0124]

<sup>944</sup> The coupon issuing member (issuer) connects online to the coupon issuing member terminal (issuer's terminal), selects a recipient (S140), and issues a coupon (S200).

[0125]

<sup>949</sup> The coupon service provider server receives coupon- related information from the coupon issuing member terminal, and delivers the coupon and coupon- related information to the recipient terminal.

[0126]

<sup>955</sup> The recipient receives the coupon and coupon- related information transmitted from the coupon service provider server through the recipient terminal (212).

<sup>957</sup> In this way, a coupon is created in the recipient's terminal.

[0127]

<sup>961</sup> Here, "online" refers to an environment in which access is made through a website or  
Petitioner Exhibit 1002-4125

program execution, and an Internet connection is provided.

963 Also, coupon generation on the recipient's terminal is executed through a program installed in the recipient's terminal.

### [0128]

968 9 is an explanatory diagram illustrating a case of issuing a coupon in a recipient terminal in the present invention.

970 This is a case where the issuer issues a coupon using the recipient's terminal.

### [0129]

974 First, a program (service) distributed by a coupon service provider is executed in the recipient's terminal, an issuer (coupon issuing member) is set using the recipient's terminal, and coupon issuance is selected from selection buttons (or selection keys).

### [0130]

981 Next, issuer authentication is performed through the recipient terminal (S120), and upon authentication, information necessary for authentication is transmitted to the coupon service provider server, and the coupon service provider server receives it.

984 That is, authentication is requested while transmitting the authentication code or ID and password or personal barcode issued by the issuer in advance to the coupon service provider server 100, and the coupon service provider server authenticates it and approves it to the recipient terminal. transmit a signal

### [0131]

991 Next, the issuer sets a goal for a specific activity through the recipient terminal, sets a reward and pays for the set reward, requests the issuance of a coupon from the recipient terminal to the coupon service provider server, and the coupon service provider server The recipient's terminal verifies whether the requested coupon is issued, transmits a coupon issuance approval signal to the recipient's terminal, and the coupon is created in the recipient's terminal.

997 In addition, the coupon service provider server stores coupon- related information on its own and transmits coupon- related information to the issuer terminal at the same time.

### [0132]

1003 In the present invention, when a coupon is issued directly from a recipient's



terminal, there are largely two methods for authenticating the issuer.

1005 The first method is when a separate authentication code or identification code is given after signing up as an existing online service (a kind of ID), and the second method is the issuer authentication method through a mobile authenticator, which is a kind of mobile OTP method. It is a method of implementing OTP as a mobile app or program and then executing it to enter the authentication code.

### [0133]

1013 10 is a flowchart of an embodiment of an issuer authentication method when directly issuing a coupon from a recipient terminal in the present invention.

1015 10 shows a case in which a separate authentication code or identification code (a kind of ID) is given after signing up as a member of an existing online service.

### [0134]

1020 10 is a case of issuing a coupon from a recipient terminal as shown in FIG. 9. For authentication used here, the issuer registers as a member of a coupon service provider in advance, but transmits information necessary for membership to the coupon service provider, After receiving this, the coupon service provider assigns an authentication code and transmits it to the issuer, and the issuer receives the authentication code.

### [0135]

1029 Then, as shown in FIG. 9, the issuer executes the program (service) distributed by the coupon service provider on the recipient's terminal, sets the issuer (coupon issuing member) using the recipient's terminal, and selects a selection button (or selection key). ), select coupon issuance.

### [0136]

1036 Then, the issuer authentication is performed through the recipient terminal, and upon authentication, an authentication code is input and the authentication code is transmitted to the coupon service provider server, and the coupon service provider server receives it.

1040 The coupon service provider server performs authentication using this and transmits an approval signal to the recipient's terminal.

### [0137]

1045 Next, the issuer sets a goal for a specific activity through the recipient terminal,

sets a reward and pays for the set reward, requests the issuance of a coupon from the recipient terminal to the coupon service provider server, and the coupon service provider server The recipient's terminal verifies whether the requested coupon is issued, transmits a coupon issuance approval signal to the recipient's terminal, and the coupon is created in the recipient's terminal.

1057 In addition, the coupon service provider server stores coupon- related information on its own, and at the same time transmits coupon- related information to the issuer terminal to create and manage a customer DB.

### [0138]

1057 11 is a flowchart of another embodiment of an issuer authentication method when directly issuing a coupon from a recipient terminal in the present invention.

1059 11 is an issuer authentication method through a mobile authenticator.

### [0139]

1063 In FIG. 11, a mobile authenticator, a program for mobile devices provided by a coupon service provider, is downloaded, executed, an identification code is checked, the identification code is registered, it is transmitted to the coupon service provider server, and the coupon service The provider server receives and stores and manages it.

### [0140]

1071 Then, as shown in FIG. 9, the issuer executes the program (service) distributed by the coupon service provider on the recipient's terminal, sets the issuer (coupon issuing member) using the recipient's terminal, and selects a selection button (or selection key). ), select coupon issuance.

### [0141]

1078 Then, issuer authentication is performed through the recipient terminal, and upon authentication, an identification code (ie, authentication code) is input and the identification code (authentication code) is transmitted to the coupon service provider server, and the coupon service provider server is the recipient terminal Receives an identification code (authentication code) from the mobile authenticator, executes the mobile authenticator, receives the authentication code, performs authentication, and transmits an approval signal to the recipient's terminal.

### [0142]

1088 Next, the issuer sets a goal for a specific activity through the recipient terminal, sets a reward and pays for the set reward, requests the issuance of a coupon from the recipient terminal to the coupon service provider server, and the coupon service provider server. The recipient's terminal verifies whether the requested coupon is issued, transmits a coupon issuance approval signal to the recipient's terminal, and the coupon is created in the recipient's terminal.

[0143]

1097 12 is an example of issuing a coupon using a recipient terminal in the personal marketing system of the present invention.

[0144]

1102 12 shows an example of an execution screen when an issuer directly creates a coupon in a coupon recipient terminal.

1104 In this case, issuance information is previously stored on the corresponding screen.

[0145]

1108 12(a) shows a screen for selecting a coupon issuance selection key to request coupon issuance to a coupon service provider server, and FIG. 12(b) shows a screen for inputting an authentication code for authentication. 12(c) shows a screen when a coupon is issued, and FIG. 12(d) shows a screen where a coupon is created in a recipient terminal.

[0146]

1116 13 is another example of issuing a coupon using a recipient terminal in the personal marketing system of the present invention.

1118 In this case, issuance information is directly input, and issuance information is not stored in advance.

[0147]

1123 13(a) shows a screen for inputting an authentication code for authentication, and FIG. 13(b) shows a screen for setting goals of a specific activity, that is, mission type, target number, expiration date, etc., through the recipient's terminal. am.

[0148]

1129 13(c) is a screen for setting rewards. In the screen of FIG. 13(c), multiple rewards

can be purchased, and the remaining rewards are stored and can be selected for shopping when the next coupon is issued.

1132 13 (b) to (c) may be fixed and registered in advance, and the corresponding step may be skipped when the coupon is issued next time.

[0149]

1137 13(d) is a screen for making a payment for a set reward.

[0150]

1141 14 is an example of screens showing coupon generation and reward reception in the personal marketing system of the present invention.

[0151]

1146 FIG. 14(a) shows a screen on which a coupon is received in the recipient's terminal, and FIG. 14(b) shows a screen on which a gift certificate is received as a reward (compensation) after the recipient completes the goal.

1149 14(b) shows that the stamp coupon of FIG. 14(a) is converted into an online gift certificate by completing the goal (mission) that the corresponding coupon must reach a predetermined number.

1152 The stamp coupon shown in (a) of FIG. 14 is automatically deleted when the goal (mission) is completed.

[0152]

1157 14(c) shows a screen in which a stamp is provided as a reward (compensation) when the recipient completes the goal, and FIG. 14(d) shows a stamp by pressing the 'confirm' button in This is the screen that shows the accumulated status.

[0153]

1163 That is, the screen of FIG. 14 (b) shows a case in which a general (online) gift certificate is paid as a reward, and the screen in FIG. 14 (c) shows a case in which a stamp of another coupon within the same service is provided as a reward.

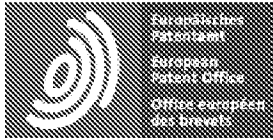
[0154]

1169 As described above, the present invention has been described by the limited embodiments and drawings, but the present invention is not limited to the above embodiments, and those skilled in the art in the field to which the present invention

belongs can make various modifications and transformation is possible  
1173 Therefore, the spirit of the present invention should be grasped only by the claims  
described below, and all equivalent or equivalent modifications thereof will be said  
to belong to the scope of the spirit of the present invention.

[0155]

1179 100: Coupon service provider server 210, 250: member terminal



# Patent Translate

Powered by EPO and Google

## Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

## CLAIMS KR20130138637A

1.

<sup>14</sup> The coupon issuing member terminal installed by receiving the service program provided by the coupon service provider stores coupon recipient information including coupon receiving member terminal information and target information for receiving a reward (compensation), temporarily storing receipt conditions. After the receipt condition storage step, the coupon issuing member terminal stores the set reward temporarily, the reward storage step; After the reward storage step, the coupon issuing member terminal performs payment for the set reward; Payment step; After the payment step, A coupon receiving step in which the issued coupon is transmitted from the coupon issuing member terminal to the coupon receiving member terminal, and at the same time, the set goal and reward information is also transmitted to the coupon receiving member terminal; either the coupon service provider server or the coupon issuing member terminal Reward receiving step of receiving the target performance result from the coupon receiving member terminal and providing a reward (compensation) to the coupon receiving member terminal when it is determined that the target performance is complete; Personal marketing method using shopping.

2.

<sup>33</sup> The coupon issuing member terminal installed by receiving the service program provided by the coupon service provider stores coupon recipient information including coupon receiving member terminal information and target information for receiving a reward (compensation), temporarily storing receipt conditions. After the receipt condition storage step, the coupon issuing member terminal stores the set reward

Petitioner Exhibit 1002-4132

temporarily; after the reward storage step, the coupon issuing member terminal performs a provisional payment for the set reward, a provisional payment step; provisional payment After the step, the coupon issuing member terminal transmits the issued coupon to the coupon receiving member terminal, and at the same time, the set goal and reward information is transmitted to the coupon receiving member terminal. Coupon receiving step; After the coupon receiving step, the coupon service provider If one of the server or the coupon issuing member terminal receives the target performance result from the coupon receiving member terminal and determines that the target performance is complete, in the provisional payment step, automatically pays the paid reward and receives the reward (compensation) as a coupon Reward receiving step provided to the member terminal; After the coupon receiving step, if one of the coupon service provider server or the coupon issuing member terminal receives the target performance result from the coupon receiving member terminal, but determines that the target performance is not completed , In the temporary payment step, a reward refund step in which the paid reward is refunded; personal marketing method using a mobile accumulated coupon and online shopping, characterized in that it is made including.

3.

<sup>58</sup> The method according to any one of claims 1 or 2, wherein at the previous stage of the receipt condition storage step, the coupon issuing member terminal has one or more of authentication codes or IDs and passwords or personal barcodes issued by coupon issuing members in advance. Authentication step of transmitting to the coupon service provider server to perform authentication; Personal marketing method using mobile coupons and online shopping characterized in that it further comprises.

4.

<sup>67</sup> According to any one of claims 1 or 2, The reward is a personal marketing method using a mobile accumulated coupon and online shopping, characterized in that the online product or coupon or gift certificate or stamp.

5.

<sup>73</sup> The mobile according to claim 4, wherein the reward is an online product or coupon, gift certificate or stamp of an online shopping mall of a member company affiliated with a coupon service provider or an online shopping mall of a member company affiliated with a coupon service provider. Personal marketing method using coupons and online shopping.

6.

<sup>87</sup> The method according to any one of claims 1 or 2, wherein in the coupon receiving step, the issued coupon is: requesting coupon issuance from the coupon issuing member terminal to the coupon service provider server; Verifying whether or not the issued coupon is issued, transmitting an approval signal for issuing the coupon to the coupon issuing member terminal, and storing coupon- related information; Personal marketing method using coupons and online shopping.

7.

<sup>90</sup> According to any one of claims 1 or 2, In the coupon receiving step, the issued coupon, points, personal marketing method using a mobile accumulated coupon and online shopping, characterized in that the accumulated coupon containing a stamp.

8.

<sup>96</sup> The payment step of claim 1, if, in the reward receiving step, one of the coupon service provider server or the coupon issuing member terminal receives the target performance result from the coupon receiving member terminal, but determines that the target performance is not completed. Personal marketing method using a mobile accumulated coupon and online shopping, characterized in that it further comprises a; reward refund step in which the reward paid in is refunded.

9.

<sup>105</sup> According to any one of claims 1 or 2, The coupon issuing member terminal is a parent's terminal, Coupon receiving member terminal is a personal marketing method using a mobile accumulated coupon and online shopping, characterized in that the terminal of the child.

10.

<sup>112</sup> The method of claim 1 or 2, wherein the coupon issuing member terminal is a terminal of a single entrepreneur, and the coupon receiving member terminal is a terminal of a customer of the single entrepreneur. Personal marketing method using .

11.

<sup>118</sup> According to any one of claims 1 or 2, The coupon issuing member terminal is a personal marketing method using a mobile accumulated coupon and online shopping, characterized in that the same as the coupon receiving member terminal.



12.

<sup>124</sup> A coupon service provider server that provides a service program (app program) for issuing mobile coupons to members and manages coupons and rewards (compensation) issued by members; Using the service program, coupon recipients, receipt conditions, A coupon issuing member terminal in which a reward (compensation) is set and a mobile accumulation coupon is issued; a coupon, receipt condition information, and reward information are received from the coupon issuing member terminal, and a reward (compensation) is issued when the goal included in the receipt condition information is completed. A personal marketing system using a mobile accumulated coupon and online shopping, characterized in that made by including; a coupon receiving member terminal to be received.

13.

<sup>137</sup> According to claim 12, Coupon issuing member terminal personal marketing system using a mobile accumulated coupon and online shopping, characterized in that made to make a payment for the set reward.

14.

<sup>143</sup> The method of claim 13, If one of the coupon service provider server or the coupon issuing member terminal receives the target performance result from the coupon receiving member terminal, but determines that the target performance is not completed, the reward paid in the payment step is A personal marketing system using mobile savings coupons and online shopping, characterized in that they are automatically refunded.

15.

<sup>152</sup> The personal marketing system of claim 13, wherein the coupon issuing member terminal is configured to make provisional payment when a reward is set.

16.

<sup>157</sup> The method of claim 15, wherein one of the coupon service provider server or the coupon issuing member terminal receives the target performance result from the coupon receiving member terminal and automatically pays the reward paid in the coupon issuing member terminal when it is determined that the target performance is complete. And a personal marketing system using a mobile accumulated coupon and online shopping, characterized in that for providing a reward (compensation) to the coupon receiving member terminal.

17.

<sup>167</sup> The method of claim 15, wherein one of the coupon service provider server or the coupon issuing member terminal receives the target performance result from the coupon receiving member terminal, but when it is determined that the target performance is not completed, the coupon issuing member terminal is paid. A personal marketing system using mobile savings coupons and online shopping, characterized in that rewards are refunded.

18.

<sup>176</sup> The method according to any one of claims 12 to 17, wherein the coupon issuing member terminal transmits one or more of the authentication code or ID and password or personal barcode issued by the coupon issuing member in advance to the coupon service provider. Personal marketing system using a mobile accumulated coupon and online shopping, characterized in that transmitted to the server to perform authentication.

19.

<sup>185</sup> According to any one of claims 12 to 17, The reward is a personal marketing system using a mobile accumulated coupon and online shopping, characterized in that the online product or coupon or gift certificate or stamp.

20.

<sup>191</sup> The method of claim 19, wherein the reward is an online shopping mall of a member company affiliated with a coupon service provider, or an online product or coupon, gift certificate, or stamp of a member company affiliated with a coupon service provider. Personal marketing system using coupons and online shopping.

21.

<sup>198</sup> According to any one of claims 12 to 17, The coupon issued by the coupon- issuing member terminal is a personal marketing system using a mobile accumulation coupon and online shopping, characterized in that the coupon is an accumulation- type coupon including points and stamps.

22.

<sup>205</sup> According to any one of claims 12 to 17, The coupon issuing member terminal is a

parent's terminal, Coupon receiving member terminal is a personal marketing system using mobile accumulated coupons and online shopping, characterized in that the terminal of the child.

23.

<sup>212</sup> According to any one of claims 12 to 17, The coupon issuing member terminal is a terminal of a single entrepreneur, and the coupon receiving member terminal is a terminal of a customer of the single entrepreneur. Personal marketing system using .



(19) 대한민국특허청(KR)  
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0138637  
(43) 공개일자 2013년12월19일

(51) 국제특허분류(Int. Cl.)  
G06Q 30/02 (2012.01)

(21) 출원번호 10-2012-0099066

(22) 출원일자 2012년09월07일

심사청구일자 없음

(30) 우선권주장

1020120061872 2012년06월11일 대한민국(KR)

(71) 출원인

주식회사 리안디지털

서울특별시 마포구 잔다리로3안길 24, 202(서교동, 라임하우스)

(72) 발명자

안대형

서울특별시 마포구 잔다리로3안길 24 202(서교동 라임하우스)

장현주

서울특별시 마포구 잔다리로3안길 24 202(서교동 라임하우스)

(74) 대리인

민혜정

전체 청구항 수 : 총 23 항

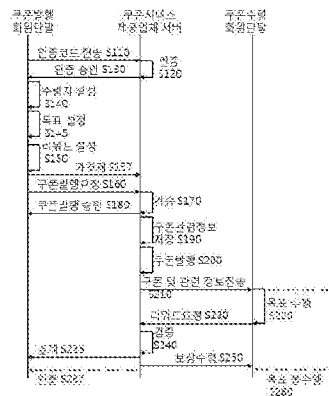
(54) 발명의 명칭 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템 및 그 방법

(57) 요약

본 발명은 쿠폰서비스 제공업체에 회원 가입된 고객이 다른 회원에게 모바일 적립쿠폰 및 리워드를 제공하는 방법으로, 서비스 이용자는 제공된 기능을 통해 모바일 적립쿠폰을 발행하고 이를 발행함과 동시에 특정 목표 수치에 도달 시 이에 상응하는 리워드(온라인 상품 혹은 상품 교환권)를 온라인 쇼핑몰에서 지정하고, 쿠폰을 제공받은 유저는 특정 활동을 통해 특정 수치에 도달하면, 해당 적립쿠폰은 자동적으로 미리 지정되어 있던 리워드로 변경되는, 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템 및 그 방법에 관한 것이다.

본 발명의 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법은, 쿠폰서비스 제공업체로부터 제공하는 서비스프로그램을 수신하여 설치된, 쿠폰 발행 회원단말기는, 쿠폰수령 회원단말기 정보를 포함하는 쿠폰 수령자 정보와, 리워드(보상)을 받기 위한 목표 정보를 임시저장하는, 수령조건 저장단계; 수령조건 저장단계 후, 쿠폰 발행 회원단말기는 설정된 리워드가 임시저장되는, 리워드 저장단계; 리워드 저장단계 후, 쿠폰발행 회원단말기에서, 설정된 리워드에 대한 가결제를 행하는, 가결제단계; 가결제단계 후, 쿠폰 발행 회원단말기에서, 발행된 쿠폰을, 쿠폰수령 회원단말기로 전송하며, 동시에 설정된 목표 및 리워드의 정보도 쿠폰수령 회원단말기로 전송되는 쿠폰 수령단계; 쿠폰 수령단계 후, 쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원단말기로부터 목표수행 결과를 수신하고 목표수행 완료로 판단되면, 상기 가결제단계에서, 가 결제된 리워드를 자동 결제하고, 리워드(보상)를 쿠폰수령 회원 단말기로 제공하는, 리워드 수령단계; 쿠폰 수령단계 후, 쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원단말기로부터 목표수행 결과를 수신하였으나, 목표수행이 완료되지 않은 것으로 판단되면, 상기 가결제단계에서, 가 결제된 리워드가 환불되는, 리워드 환불단계;를 포함하여 이루어진 것을 특징으로 한다.

도면 - 도4



**특허청구의 범위**

**청구항 1**

쿠폰서비스 제공업체로부터 제공하는 서비스프로그램을 수신하여 설치된, 쿠폰 발행 회원단말기는, 쿠폰수령 회원단말기 정보를 포함하는 쿠폰 수령자 정보와, 리워드(보상)을 받기 위한 목표 정보를 임시저장하는, 수령조건 저장단계;

수령조건 저장단계 후, 쿠폰 발행 회원단말기는 설정된 리워드가 임시저장되는, 리워드 저장단계;

리워드 저장단계 후, 쿠폰발행 회원 단말기에서, 설정된 리워드에 대한 결제를 행하는, 결제단계;

결제단계 후, 쿠폰 발행 회원단말기에서, 발행된 쿠폰을, 쿠폰수령 회원단말기로 전송하며, 동시에 설정된 목표 및 리워드의 정보도 쿠폰수령 회원단말기로 전송되는 쿠폰 수령단계;

쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원단말기로부터 목표수행 결과를 수신하고 목표수행 완료로 판단되면, 리워드(보상)를 쿠폰수령 회원 단말기로 제공하는, 리워드 수령단계;

를 포함하여 이루어진 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법.

**청구항 2**

쿠폰서비스 제공업체로부터 제공하는 서비스프로그램을 수신하여 설치된, 쿠폰 발행 회원단말기는, 쿠폰수령 회원단말기 정보를 포함하는 쿠폰 수령자 정보와, 리워드(보상)을 받기 위한 목표 정보를 임시저장하는, 수령조건 저장단계;

수령조건 저장단계 후, 쿠폰 발행 회원단말기는 설정된 리워드가 임시저장되는, 리워드 저장단계;

리워드 저장단계 후, 쿠폰발행 회원 단말기에서, 설정된 리워드에 대한 가결제를 행하는, 가결제단계;

가결제단계 후, 쿠폰 발행 회원단말기에서, 발행된 쿠폰을, 쿠폰수령 회원단말기로 전송하며, 동시에 설정된 목표 및 리워드의 정보도 쿠폰수령 회원단말기로 전송되는 쿠폰 수령단계;

쿠폰 수령단계 후, 쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원단말기로부터 목표수행 결과를 수신하고 목표수행 완료로 판단되면, 상기 가결제단계에서, 가 결제된 리워드를 자동 결제하고, 리워드(보상)를 쿠폰수령 회원 단말기로 제공하는, 리워드 수령단계;

쿠폰 수령단계 후, 쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원단말기로부터 목표수행 결과를 수신하였으나, 목표수행이 완료되지 않은 것으로 판단되면, 상기 가결제단계에서, 가 결제된 리워드가 환불되는, 리워드 환불단계;

를 포함하여 이루어진 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법.

**청구항 3**

제1항 또는 제2항 중 어느 한 항에 있어서,

수령조건 저장단계의 전 단계, 쿠폰발행 회원 단말기는, 쿠폰 발행 회원이 사전에 발급받은 인증코드 혹은 아이디와 암호 또는 개인 바코드 들 중의 하나 이상을 쿠폰서비스 제공업체 서버로 전송하여 인증을 행하는 인증단계; 를 더 포함하는 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법.

**청구항 4**

제1항 또는 제2항 중 어느 한 항에 있어서,

리워드는 온라인 상품 또는 쿠폰 또는 상품권 또는 스탬프인 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법.

**청구항 5**

제4항에 있어서,

리워드는, 쿠폰서비스 제공업체에 가입된 회원사의 온라인 쇼핑물, 또는 쿠폰서비스 제공업체와 제휴를 맺은 회원사의 온라인 쇼핑물의, 온라인 상품 또는 쿠폰 또는 상품권 또는 스탬프인 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법.

#### 청구항 6

제1항 또는 제2항 중 어느 한 항에 있어서,

쿠폰 수령단계에서, 발행된 쿠폰은,

쿠폰발행 회원 단말기에서, 쿠폰서비스 제공업체 서버로 쿠폰 발행을 요청하는 단계;

쿠폰서비스 제공업체 서버는 요청된 쿠폰발행 여부를 검증하고 쿠폰발행의 승인 신호를 쿠폰발행 회원 단말기로 전송하고, 쿠폰관련정보를 저장하는 단계;

쿠폰발행 회원 단말기는 쿠폰을 발행하는 단계;

를 포함하여 이루어진 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법.

#### 청구항 7

제1항 또는 제2항 중 어느 한 항에 있어서,

쿠폰 수령단계에서, 발행된 쿠폰은,

포인트, 스탬프를 포함하는 적립식의 쿠폰인 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법.

#### 청구항 8

제1항에 있어서,

리워드 수령단계에서, 쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원단말기로부터 목표수행 결과를 수신하였으나, 목표수행이 완료되지 않은 것으로 판단되면, 상기 결제단계에서 결제한 리워드가 환불이 되는 리워드 환불단계;

를 더 포함하는 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법.

#### 청구항 9

제1항 또는 제2항 중 어느 한 항에 있어서,

쿠폰 발행 회원단말기는 부모의 단말기이며,

쿠폰수령 회원 단말기는 자녀의 단말기인 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법.

#### 청구항 10

제1항 또는 제2항 중 어느 한 항에 있어서,

쿠폰 발행 회원단말기는 1인 기업인의 단말기이며,

쿠폰수령 회원 단말기는 상기 1인 기업인의 고객의 단말기인 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법.

#### 청구항 11

제1항 또는 제2항 중 어느 한 항에 있어서,

쿠폰 발행 회원단말기는 쿠폰수령 회원 단말기와 동일한 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법.

**청구항 12**

회원들에게 모바일 쿠폰을 발행하는 서비스 프로그램(앱 프로그램)을 제공하고, 회원이 발행한 쿠폰 및 리워드(보상)를 관리하는 쿠폰서비스 제공업체 서버;

상기 서비스 프로그램을 이용하여, 쿠폰수령자, 수령조건, 리워드(보상)가 설정되고, 모바일 적립쿠폰이 발행되는 쿠폰 발행 회원단말기;

쿠폰 발행 회원단말기로부터 쿠폰, 수령조건 정보, 리워드 정보를 수신하고, 수령조건 정보에 포함된 목표가 완료되면 리워드(보상)를 수신하게 되는 쿠폰수령 회원 단말기;

를 포함하여 이루어진 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템.

**청구항 13**

제12항에 있어서,

쿠폰 발행 회원단말기는 설정된 리워드에 대한 결제를 행하도록 이루어진 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템.

**청구항 14**

제13항에 있어서,

쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원단말기로부터 목표수행 결과를 수신하였으나, 목표수행이 완료되지 않은 것으로 판단되면, 상기 결제단계에서 결제한 리워드가 자동으로 환불되는 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템.

**청구항 15**

제13항에 있어서,

쿠폰발행 회원 단말기는 리워드가 설정되면 가결제를 행하도록 이루어진 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템.

**청구항 16**

제15항에 있어서,

쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원단말기로부터 목표수행 결과를 수신하고 목표수행 완료로 판단되면, 쿠폰발행 회원 단말기에서 가 결제된 리워드를 자동 결제하고, 리워드(보상)를 쿠폰수령 회원 단말기로 제공하는 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템.

**청구항 17**

제15항에 있어서,

쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원단말기로부터 목표수행 결과를 수신하였으나, 목표수행이 완료되지 않은 것으로 판단되면, 쿠폰발행 회원 단말기에서 가 결제된 리워드가 환불되는 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템.

**청구항 18**

제12항 내지 제17항 중 어느 한 항에 있어서,

쿠폰발행 회원 단말기는, 쿠폰발행전에, 쿠폰 발행 회원이 사전에 발급받은 인증코드 혹은 아이디와 암호 또는 개인 바코드 들 중의 하나 이상을 쿠폰서비스 제공업체 서버로 전송하여 인증을 행하도록 이루어진 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템.

**청구항 19**

제12항 내지 제17항 중 어느 한 항에 있어서,

리워드는 온라인 상품 또는 쿠폰 또는 상품권 또는 스탬프인 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템.

**청구항 20**

제19항에 있어서,

리워드는, 쿠폰서비스 제공업체에 가입된 회원사의 온라인 쇼핑물, 또는 쿠폰서비스 제공업체와 제휴를 맺은 회원사의 온라인 쇼핑물의, 온라인 상품 또는 쿠폰 또는 상품권 또는 스탬프인 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템.

**청구항 21**

제12항 내지 제17항 중 어느 한 항에 있어서,

쿠폰발행 회원 단말기에서 발행된 쿠폰은,

포인트, 스탬프를 포함하는 적립식의 쿠폰인 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템.

**청구항 22**

제12항 내지 제17항 중 어느 한 항에 있어서,

쿠폰 발행 회원단말기는 부모의 단말기이며,

쿠폰수령 회원 단말기는 자녀의 단말기인 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템.

**청구항 23**

제12항 내지 제17항 중 어느 한 항에 있어서,

쿠폰 발행 회원단말기는 1인 기업인의 단말기이며,

쿠폰수령 회원 단말기는 상기 1인 기업인의 고객의 단말기인 것을 특징으로 하는 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템.

**명세서**

**기술분야**

[0001] 본 발명은 모바일 적립쿠폰(적립금, 적립 포인트, 스탬프 등)과 온라인 쇼핑을 이용하여 개인별 고객관리하는 퍼스널 마케팅 시스템 및 그 방법에 관한 것이다. 보다 상세하게는 본 발명은, 쿠폰서비스 제공업체에 회원 가입된 고객의 이동통신단말기에 모바일 쿠폰을 제공하는 기능을 제공하고 이를 활용하여 회원은 해당 서비스를 이용하는 다른 회원에게 모바일 적립쿠폰 및 리워드(reward, 보상)를 제공하는 방법으로, 서비스 이용자는 제공된 기능을 통해 모바일 적립쿠폰을 발행하고 이를 발행함과 동시에 특정 목표 수치에 도달 시 이에 상응하는 리워드(온라인 상품 혹은 상품 교환권)를 온라인 쇼핑물에서 지정하고, 쿠폰을 제공받은 유저는 특정 활동을 통해 특정 수치에 도달하면, 해당 적립쿠폰은 자동적으로 미리 지정되어 있던 리워드로 변경되는, 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템 및 그 방법에 관한 것이다.

**배경기술**

[0002] 현대는 퍼스널 브랜드 시대로, 1인 기업 및 개인 브랜드가 부각되고 있으며, 마케팅은 더 이상 기업과 상점에 한한 활동이 아니다. SNS와 스마트폰으로 소통함에 따라 개개인의 네임밸류와 사회적 위치, 관계, 인맥 등은 더욱더 중요해지고 있다.

[0003] 특히, 모바일단말기의 비약적인 보급과 비례하여 모바일 쿠폰의 사용이 증가되었으며 문화적으로도 휴대가 간편하고 사용이 편리한 지불수단의 한가지 형태로 자리 잡혀 가고 있다.



[0004] 종래에, 수많은 인프라가 필요한 기존 마케팅에서는, 1인 기업, 개개인의 마케팅이 어려웠던 것에 비해, 현재는 모바일 앱을 통해 1인 기업, 개개인의 마케팅이 손쉬워 졌으며, 특히, 모바일 앱을 통한 여러 서비스의 출현과 모바일 광고, 쿠폰 등을 이용하여, 보다 쉽고 효과적인 마케팅 활동이 가능하게 되었다. 이에 따라 스마트폰을 활용하여 보다 간단하고 편리한 퍼스널 마케팅 방법이 요망되었다.

[0005] 따라서, 본 발명은 모바일 적립쿠폰(적립금, 적립 포인트, 스탬프 등)과 온라인 쇼핑을 이용하여 개인별 고객관리하는 퍼스널 마케팅 시스템 및 그 방법을 제안한다.

[0006] 본 발명은 쿠폰서비스 제공업체에 회원 가입된 고객의 이동통신단말기에 모바일 쿠폰을 제공하는 기능을 제공하고, 이를 활용하여 회원은 해당 서비스를 이용하는 다른 회원에게 모바일 적립쿠폰 및 리워드를 제공하는 방법이다. 본 발명에서 서비스 이용자는 제공된 기능을 통해 모바일 적립쿠폰을 발행하고 이를 발행함과 동시에 특정 목표 수치에 도달 시 이에 상응하는 리워드(온라인 상품 혹은 상품 교환권)를 지정한 온라인 쇼핑물 혹은 서비스 내에서 지정, 쿠폰을 제공받은 유저는 특정 활동을 통해 특정 수치에 도달, 해당 적립쿠폰은 자동적으로 미리 지정되어 있던 리워드로 변경된다.

*발명의 내용*

*해결하려는 과제*

[0007] 본 발명이 해결하고자 하는 과제는, 쿠폰서비스 제공업체에 회원 가입된 고객의 이동통신단말기에 모바일 쿠폰을 제공하는 기능을 제공하고, 이를 활용하여 회원은 해당 서비스를 이용하는 다른 회원에게 모바일 적립쿠폰 및 리워드를 제공하는, 모바일 적립쿠폰(적립금, 적립 포인트, 스탬프 등)과 온라인 쇼핑을 이용하여 개인별 고객관리하는 퍼스널 마케팅 시스템 및 그 방법을 제공하는 것이다.

[0008] 본 발명이 해결하고자 하는 다른 과제는, 서비스 이용자는 제공된 기능을 통해 모바일 적립쿠폰을 발행하고 이를 발행함과 동시에 특정 목표 수치에 도달 시 이에 상응하는 리워드(온라인 상품 혹은 상품 교환권)를 온라인 쇼핑물 혹은 서비스 내에서 지정하며, 쿠폰을 제공받은 유저는 특정 활동을 통해 특정 수치에 도달하면, 해당 적립쿠폰은 자동적으로 미리 지정되어 있던 리워드로 변경되는, 모바일 적립쿠폰(적립금, 적립 포인트, 스탬프 등)과 온라인 쇼핑을 이용하여 개인별 고객관리하는 퍼스널 마케팅 시스템 및 그 방법을 제공하는 것이다.

*과제의 해결 수단*

[0009] 상기 과제를 해결하기 위해, 본 발명의 제1실시에에 의한 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법은, 쿠폰서비스 제공업체로부터 제공하는 서비스프로그램을 수신하여 설치된, 쿠폰 발행 회원단말기는, 쿠폰수령 회원단말기 정보를 포함하는 쿠폰 수령자 정보와, 리워드(보상)을 받기 위한 목표 정보를 임시저장하는, 수령조건 저장단계; 수령조건 저장단계 후, 쿠폰 발행 회원단말기는 설정된 리워드가 임시저장되는, 리워드 저장단계; 리워드 저장단계 후, 쿠폰발행 회원 단말기에서, 설정된 리워드에 대한 결제를 행하는, 결제단계; 결제단계 후, 쿠폰 발행 회원단말기에서, 발행된 쿠폰을, 쿠폰수령 회원단말기로 전송하며, 동시에 설정된 목표 및 리워드의 정보도 쿠폰수령 회원단말기로 전송되는 쿠폰 수령단계; 쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원단말기로부터 목표수행 결과를 수신하고 목표수행 완료로 판단되면, 리워드(보상)를 쿠폰수령 회원 단말기로 제공하는, 리워드 수령단계;를 포함하여 이루어진 것을 특징으로 한다.

[0010] 본 발명의 제2실시에에 의한 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법은, 쿠폰서비스 제공업체로부터 제공하는 서비스프로그램을 수신하여 설치된, 쿠폰 발행 회원단말기는, 쿠폰수령 회원단말기 정보를 포함하는 쿠폰 수령자 정보와, 리워드(보상)을 받기 위한 목표 정보를 임시저장하는, 수령조건 저장단계; 수령조건 저장단계 후, 쿠폰 발행 회원단말기는 설정된 리워드가 임시저장되는, 리워드 저장단계; 리워드 저장단계 후, 쿠폰발행 회원 단말기에서, 설정된 리워드에 대한 가결제를 행하는, 가결제단계; 가결제단계 후, 쿠폰 발행 회원단말기에서, 발행된 쿠폰을, 쿠폰수령 회원단말기로 전송하며, 동시에 설정된 목표 및 리워드의 정보도 쿠폰수령 회원단말기로 전송되는 쿠폰 수령단계; 쿠폰 수령단계 후, 쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원단말기로부터 목표수행 결과를 수신하고 목표수행 완료로 판단되면, 상기 가결제단계에서, 가 결제된 리워드를 자동 결제하고, 리워드(보상)를 쿠폰수령 회원 단말기로 제공하는, 리워드 수령단계;쿠폰 수령단계 후, 쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원 단말기로부터 목표수행 결과를 수신하였으나, 목표수행이 완료되지 않은 것으로 판단되면, 상기 가결제단계에서, 가 결제된 리워드가 환불되는, 리워드 환불단계;를 포함하여 이루어진 것을 특징으로 한다.

- [0011] 수령조건 저장단계의 전 단계, 쿠폰발행 회원 단말기는, 쿠폰 발행 회원이 사전에 발급받은 인증코드 혹은 아이디와 암호 또는 개인 바코드 들 중의 하나 이상을 쿠폰서비스 제공업체 서버로 전송하여 인증을 행하는 인증단계; 를 더 포함한다.
- [0012] 리워드는 온라인 상품 또는 쿠폰 또는 상품권 또는 스탬프이며, 특히, 리워드는, 쿠폰서비스 제공업체에 가입된 회원사의 온라인 쇼핑물, 또는 쿠폰서비스 제공업체와 제휴를 맺은 회원사의 온라인 쇼핑물의, 온라인 상품 또는 쿠폰 또는 상품권 또는 스탬프일 수 있다.
- [0013] 쿠폰 수령단계에서, 발행된 쿠폰은, 쿠폰발행 회원 단말기에서, 쿠폰서비스 제공업체 서버로 쿠폰 발행을 요청하는 단계; 쿠폰서비스 제공업체 서버는 요청된 쿠폰발행 여부를 검증하고 쿠폰발행의 승인 신호를 쿠폰발행 회원 단말기로 전송하고, 쿠폰관련정보를 저장하는 단계; 쿠폰발행 회원 단말기는 쿠폰을 발행하는 단계;를 포함하여 이루어진다.
- [0014] 쿠폰 수령단계에서, 발행된 쿠폰은, 포인트, 스탬프를 포함하는 적립식의 쿠폰일 수 있다.
- [0015] 제1실시예는, 리워드 수령단계에서, 쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원단말기로부터 목표수행 결과를 수신하였으나, 목표수행이 완료되지 않은 것으로 판단되면, 상기 결제단계에서 결제한 리워드가 환불이 되는 리워드 환불단계;를 더 포함한다.
- [0016] 본 발명에서 쿠폰 발행 회원단말기는 부모의 단말기이며, 쿠폰수령 회원 단말기는 자녀의 단말기일 수 있다.
- [0017] 본 발명에서 쿠폰 발행 회원단말기는 1인 기업인의 단말기이며, 쿠폰수령 회원 단말기는 상기 1인 기업인의 고객의 단말기일 수 있다.
- [0018] 본 발명에서 쿠폰 발행 회원단말기는 쿠폰수령 회원 단말기와 동일할 수 있다.
- [0019] 또한, 본 발명의 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템은, 회원들에게 모바일 쿠폰을 발행하는 서비스 프로그램(앱 프로그램)을 제공하고, 회원이 발행한 쿠폰 및 리워드(보상)를 관리하는 쿠폰서비스 제공업체 서버; 상기 서비스 프로그램을 이용하여, 쿠폰수령자, 수령조건, 리워드(보상)가 설정되고, 모바일 적립쿠폰이 발행되는 쿠폰 발행 회원단말기; 쿠폰 발행 회원단말기로부터 쿠폰, 수령조건 정보, 리워드 정보를 수신하고, 수령조건 정보에 포함된 목표가 완료되면 리워드(보상)를 수신하게 되는 쿠폰수령 회원 단말기;를 포함하여 이루어진 것을 특징으로 한다.
- [0020] 쿠폰 발행 회원단말기는 설정된 리워드에 대한 결제를 행하도록 이루어지며, 쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원단말기로부터 목표수행 결과를 수신하였으나, 목표수행이 완료되지 않은 것으로 판단되면, 상기 결제단계에서 결제한 리워드가 자동으로 환불된다.
- [0021] 쿠폰발행 회원 단말기는 리워드가 설정되면 가결제를 행하도록 이루어진다.
- [0022] 쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원단말기로부터 목표수행 결과를 수신하고 목표수행 완료로 판단되면, 쿠폰발행 회원 단말기에서, 가 결제된 리워드를 자동 결제하고, 리워드(보상)를 쿠폰수령 회원 단말기로 제공한다.
- [0023] 쿠폰서비스 제공업체 서버 또는 쿠폰 발행 회원단말기 중의 하나는, 쿠폰수령 회원단말기로부터 목표수행 결과를 수신하였으나, 목표수행이 완료되지 않은 것으로 판단되면, 쿠폰발행 회원 단말기에서, 가 결제된 리워드가 환불된다.

**발명의 효과**

- [0024] 본 발명의 모바일 적립쿠폰(적립금, 적립 포인트, 스탬프 등)과 온라인 쇼핑을 이용하여 개인별 고객관리하는 퍼스널 마케팅 시스템 및 그 방법에 따르면, 쿠폰서비스 제공업체에 회원 가입된 고객의 이동통신단말기에 모바일 쿠폰을 제공하는 기능을 제공하고, 이를 활용하여 회원은 해당 서비스를 이용하는 다른 회원에게 모바일 적립쿠폰 및 리워드를 제공한다.
- [0025] 또한, 본 발명은, 서비스 이용자는 제공된 기능을 통해 모바일 적립쿠폰을 발행하고, 이를 발행함과 동시에 특정 목표 수치에 도달 시 이에 상응하는 리워드(온라인 상품 혹은 상품 교환권)를 온라인 쇼핑물에서 지정하고, 쿠폰을 제공받은 유저는 특정 활동을 통해 특정 수치에 도달하면, 해당 적립쿠폰은 자동적으로 미리 지정되어 있던 리워드로 변경된다.

- [0026] 본 발명은, 1인 기업과 부모와 자식간의 관계 등에서 교육적인 목표로 사용할 수 있다.
- [0027] 예를 들어 부모가 자녀에게 모바일 쿠폰을 발행하면서 소정 목표치를 리워드로 제시하고, 자녀는 소정 목표치를 달성함에 의해 리워드를 수령할 수 있다.
- [0028] 다른 예로서, 1인 기업인이 자신의 고객에게 쿠폰을 발행하여, 고객 마케팅에 이용할 수 있다.

*도면의 간단한 설명*

- [0029] 도 1은 본 발명의 일 실시예에 의한 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템을 개략적으로 설명하는 설명도이다.
- 도 2는 본 발명의 일 실시예에 의한 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법에서의 서비스의 구조를 구조를 간략히 설명하기 위한 설명도이다.
- 도 3는 본 발명의 일 실시예에 의한 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법을 개략적으로 설명하는 흐름도이다.
- 도 4은 본 발명의 다른 일 실시예에 의한 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법을 개략적으로 설명하는 흐름도이다.
- 도 5는 본 발명의 또 다른 일 실시예에 의한 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법을 개략적으로 설명하는 흐름도이다.
- 도 6은 본 발명의 일 실시예에 의한 리워드 결제 및 전달을 설명하기위한 흐름도이다.
- 도 7은 본 발명의 다른 일 실시예에 의한 리워드 결제 및 전달을 설명하기위한 흐름도이다.
- 도 8은 본 발명에서 쿠폰발행 회원 단말기를 통해 쿠폰을 발행하는 경우를 설명하는 설명도이다.
- 도 9는 본 발명에서 수령자 단말기에서 쿠폰을 발행하는 경우를 설명하는 설명도이다.
- 도 10은 본 발명에서 수령자 단말기에서 직접 쿠폰 발행 시 발행자 인증방법의 일 실시예의 흐름도이다.
- 도 11은 본 발명에서 수령자 단말기에서 직접 쿠폰 발행 시 발행자 인증방법의 다른 실시예의 흐름도이다. 도 11은 모바일 인증기를 통한 발행자 인증방법이다.
- 도 12는 본 발명의 퍼스널 마케팅 시스템에서 수령자 단말기를 이용하여 쿠폰 발행시의 일예이다.
- 도 13은 본 발명의 퍼스널 마케팅 시스템에서 수령자 단말기를 이용하여 쿠폰 발행시의 다른 일예이다.
- 도 14는 본 발명의 퍼스널 마케팅 시스템에서 쿠폰의 생성 및 리워드 수신을 나타내는 화면들의 예이다.

*발명을 실시하기 위한 구체적인 내용*

- [0030] 이하, 본 발명의 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템 및 그 방법을 첨부된 도면을 참조하여 상세히 설명한다.
- [0031] 도 1은 본 발명의 일 실시예에 의한 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 시스템을 개략적으로 설명하는 설명도이다.
- [0032] 쿠폰서비스 제공업체 서버(100)는, 인증 등을 통해 가입된 회원들의 이동통신단말기, 즉, 회원 단말기(210, 250)로 모바일 쿠폰을 제공하는 기능을 가진 서비스 프로그램(앱 프로그램)을 제공하고, 회원 단말기(210, 250)들에서 발행한 쿠폰을 관리한다.
- [0033] 회원 단말기(210)는 상기 서비스 프로그램을 이용하여, 다른 회원 단말기(250)로 모바일 적립쿠폰 및 리워드를 제공한다. 회원은 회원 단말기(210)에서 상기 서비스 프로그램의 제공된 기능을 통해 모바일 적립쿠폰이 발행하고, 이와 동시에 특정 목표 수치에 도달 시 제공되는 이에 상응하는 리워드를 온라인 쇼핑물에서 지칭한다. 리워드는 온라인 상품 혹은 상품 교환권일 수 있다.
- [0034] 쿠폰을 제공받은 다른 회원 단말기(250)에서 특정 활동을 통해 특정 수치에 도달하면, 해당 적립쿠폰은 자동적으로 미리 지칭되어 있던 리워드로 변경된다. 여기서, 특정 목표 수치에 도달하는 여부는 쿠폰서비스 제공업체 서버를 통해서 체크될 수 있다.

- [0035] 본 발명의 퍼스널 마케팅 시스템에서의 서비스는, 모바일 기기를 통한 쿠폰발행으로, 이를 온라인 쇼핑과 연계하여 적립쿠폰의 리워드를 직접 선택하는 방법이다. 모바일 적립쿠폰은 이용자가 일정 목표치에 도달하면 해당 쿠폰이 자동적으로 사전에 쿠폰 발행자가 지정한 리워드 상품 혹은 상품과 교환할 수 있는 상품권으로 변경된다.
- [0036] 여기서, 본 발명에서 사용되는 용어를 설명하면 다음과 같다.
- [0037] 쿠폰의 발행이란 특정한 인증코드나 발행자의 관련 정보 입력등을 통해 쿠폰 수신자의 단말기에 해당 발행자의 쿠폰이 생성된 것을 말하며, 쿠폰의 발행시 회원의 단말기로부터 제공업체의 서버로 쿠폰정보(즉, 쿠폰의 발행 시기, 유효기간, 쿠폰의 종류(스탬프 또는 포인트 등), 목표(미션)와 리워드, 회원정보(전화번호, 이름 혹은 아이디 혹은 단말기 식별코드)를 전달한다. 특히, 본 발명에서는 쿠폰의 발행은 기본적으로 회원이 직접 타 회원에게 발행하는 것을 원칙으로 하며, 다만 쿠폰의 규칙 같은 일정한 룰에 대해서는 쿠폰 서비스 제공업체의 승인이 필요할 수도 있다.
- [0038] 목표수치는 어떤 일정한 수치에 도달하는 것으로써, 예를 들면 스탬프의 수나 포인트의 수치, 혹은 매장 방문의 횟수, 발행자와의 만남의 수 등이 될 수도 있다.
- [0039] 본 발명에서는 쿠폰의 발행수와 리워드 수는 항상 일치해야 한다.
- [0040] 리워드의 설정이란, 해당 쿠폰 서비스 업체가 직접 서비스 내 구축한 쇼핑물이나 혹은 연계한 업체의 타 서비스 판매처(쉽게 설명하면 온라인 쇼핑물)에서 관련 물품 혹은 온라인 물품을 선택하여 결제를 하는 것을 말한다.
- [0041] 일반적으로 리워드를 설정할 때는 두 가지 방법이 있다.
- [0042] 그 첫번째는 발행자가 사전에 쿠폰의 규칙을 지정하되, 쿠폰규칙 지정시에 리워드를 선정(구매)하는 경우로, 차후 설정된 리워드의 내에서 기설정된 쿠폰규칙에 따라 쿠폰을 발행하여 사용한다. 이 경우는 발행자=쿠폰규칙의 등식이 성립하며, 발행자가 발행하는 쿠폰의 리워드가 모두 동일하다면, 리워드 수와 쿠폰 발행 가능 수는 같다 (리워드 수= 쿠폰 발행 가능 수). 예를들어, 리워드를 5개 구매한 경우 발행자는 5장의 쿠폰만 발행할 수 있다.
- [0043] 두번째로, 발행자가 쿠폰의 발행마다 쿠폰의 규칙을 지정하는 경우로, 발행자는 리워드를 쿠폰 발행 시마다 결제해야 한다. 이 경우는 수신자=쿠폰규칙의 등식이 성립하는 경우로, 발행자가 쿠폰 수신자 단말기에 혹은 온라인으로 수신자 선택 후(원격발행) 쿠폰을 발행할 때마다 쿠폰을 다르게 만들어 줄 수 있는 것으로 해당 경우에는 쿠폰을 발행할 때마다 쿠폰의 규칙을 생성하게 되고 이 경우 리워드는 수신자마다 다르게 지정될 수 있다.
- [0044] 또한, 기존에 리워드를 미리 결제하거나 환불하여 남아있는 경우 별도 결제 없이 자신의 리워드 목록에서 리워드를 설정할 수 있다.
- [0045] 설정된 목표수행이란, 쿠폰의 수신자가, 발행자가 정한 기간 내에 목표에 도달하면(예를 들면 스탬프 10개를 찍는 것이 목표라면 10개를 다 찍는 것을 목표 수행이라 한다) 목표 수행으로 본다.
- [0046] 설정된 목표 불 수행은 정해진 기간 내에 목표에 도달하지 못하거나 목표에 도달했어도 기간이 지난 경우에는 목표에 불 수행이라고 보며 수신자가 쿠폰을 직접 사제하거나 해당 서비스 프로그램을 사제한 경우에도 불 수행이라고 본다.
- [0047] 본 발명에서 목표의 수행판단은 두 가지에 의해 판단할 수 있다.
- [0048] 그, 첫번째가 수치대조로써, 일정한 기간을 두고 서버가 수신자의 수치와 목표치의 수를 대조하고 유효기간을 체크하여 미션의 수행을 판단하는 경우이다.
- [0049] 두번째로, 정해진 기간 내에 목표가 수치를 완료하면 수신자의 쿠폰에 '리워드 받기' 혹은 '미션완료' 등의 버튼이 활성화 혹은 생성되고(첫번째의 수치대조의 서버체크 프로세스 통해), 수신자가 이 버튼을 클릭하면 서버가 관련 정보를 체크하여 이상이 없는 경우 미션을 완료하는 것으로 보고 리워드를 제공(해당 쿠폰이 삭제되고 리워드로 교체)하는 경우이다.
- [0050] 세번째로, 수치와 상관없이 (서버가 별도 체크하지 않음) 쿠폰에 '미션완료' 혹은 '리워드 받기' 버튼을 넣고 해당 버튼을 클릭했을 때 첫번째의 수치대조의 프로세스를 서버가 진행하고 정보일치시 미션완료, 정보 불일치시 미션 불이행으로 확인한다.
- [0051] 본 발명에서 쿠폰서비스 제공업체 서버의 역할은, 크게 정보송신 및 수신, 그리고 정보 생성이라 할 수 있다. 여기서의 정보송신 및 수신은, 첫째로, 쿠폰의 발행자와 수신자의 쿠폰 정보 연동, 둘째로, 쿠폰의 규칙이 미리 생성 시 사전에 정의된 규칙 전송 및 실행, 셋째로, 발행자의 인증정보 전송, 수신 및 일치여부 판단을 행하는

것이다. 여기서의 정보 생성은 발행자와 수신자의 쿠폰 정보 생성 및 연봉을 행하는 것을 말한다.

- [0052] 도 2는 본 발명의 일 실시예에 의한 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법에서의 서비스의 구조를 구조를 간략히 설명하기 위한 설명도이다.
- [0053] 실행단계로, 본 서비스프로그램을 설치하여 실행한다(S10).본 발명의 서비스의 실행은 스마트폰을 포함하여 앱을 실행할 수 있는 모든 모바일 기기, 온라인을 포함한다.
- [0054] 가입단계로, 설치된 서비스 프로그램을 통하여 회원 가입을 한다(S20).
- [0055] 수령자선택단계로, 쿠폰을 발행하고자 하는 회원은, 쿠폰발행 회원 단말기 에서, 쿠폰을 받을 수령자를 설정한다(S140). 쿠폰 수령자 선택이 있어서, 쿠폰을 발행하는 회원의 단말기(디바이스)에서 수령자 선택이 가능하며, 경우에 따라서 수령자의 단말기에서 직접 쿠폰 발행도 가능하다. 수령자의 단말기에서 직접 발행 시 별도의 수령자 선택 단계는 필요 없다.
- [0056] 조건입력단계로, 쿠폰발행 회원 단말기에서, 특정활동의 목표를 설정한다(S145). 즉, 쿠폰발행 회원 단말기로부터 쿠폰정보(규칙)을 쿠폰서비스 제공업체 서버로 전송하고, 쿠폰서비스 제공업체 서버는 이를 수신한다.
- [0057] 리워드 선택단계로, 쿠폰발행 회원 단말기에서, 리워드를 설정한다(S150). 따라서, 쿠폰서비스 제공업체 서버는 설정된 리워드에 대해 쿠폰발행 회원 단말기로 결제요청을 행한다.
- [0058] 결제단계로, 설정된 리워드에 대한 결제를 행한다(S155). 즉, 회원은 쿠폰발행 회원 단말기를 통해 결제정보를 전송하여 리워드를 구매하며, 쿠폰서비스 제공업체 서버는 결제를 확인한다.
- [0059] 쿠폰발행 단계로, 쿠폰발행 회원 단말기(210)에서, 쿠폰서비스 제공업체 서버(100)를 통하거나 아니면, 직접 쿠폰을 발행한다(S200). 수령자의 단말기(250)에서 직접 발행한다.
- [0060] 여기서, 회원이 쿠폰서비스 제공업체 서버에 쿠폰발행을 요청하고 쿠폰서비스 제공업체 서버가 타회원에게 발행하는 경우, 회원(발행자)이 쿠폰의 규칙(즉 쿠폰의 내용)을 입력하여 쿠폰서비스 제공업체 서버에 온라인으로 접수하고(해당 웹사이트 혹은 해당 프로그램) 이에 대한 내용을 쿠폰서비스 제공업체 서버가 검토하여 승인할 수 있다. 또한, 쿠폰을 회원이 타회원에게 직접 발행하는 것일 경우, 두 가지 방법이 있을 수 있다. 하나는, 온라인(웹사이트 혹은 프로그램)으로 회원을 검색하여 쿠폰을 원격으로 발행하는 경우이고, 다른 하나는, 수신하는 회원의 단말기에 특정 버튼을 눌러 인증코드나 발행자만의 특정 정보를 입력하여 쿠폰을 생성 발행하는 경우이다.
- [0061] 쿠폰 수령단계로, 쿠폰서비스 제공업체 서버(100) 또는 쿠폰발행 회원 단말기에서 쿠폰수령 회원 단말기로, 발행된 쿠폰이 전송된다(S210).
- [0062] 목표수행 단계로, 쿠폰을 수신한 쿠폰수령 회원은 쿠폰수령 회원 단말기를 통해 목표 수행을 행한다(S220).
- [0063] 보상수령단계로, 목표수행 단계에서 목표 수행을 완료하면, 리워드(보상)을 쿠폰수령 회원 단말기로 제공하여(S250), 결과적으로 쿠폰을 리워드로 변경한다. 즉, 쿠폰 서비스 제공업체 서버가 관련 목표치에 대해 타회원의 최종수행 목표수치와 발행자의 설정 목표수치가 동일한 경우라고 판단하면(쿠폰 서비스 제공업체 서버에서 확인이 원칙) 리워드가 전송된다.
- [0064] 본 발명에서, 리워드는 쿠폰서비스 제공업체가 타회원에게 제공한다. 리워드를 구매하면 그 리워드를 쿠폰서비스 업체가 임시로 보유하고 있다가 목표 수행시 전달하는 개념이다.
- [0065] 도 3는 본 발명의 일 실시예에 의한 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법을 개략적으로 설명하는 흐름도이다.
- [0066] 회원(210)은 모바일 쿠폰발행 해당 서비스에 가입하고, 모바일 쿠폰발행 해당 서비스에서 제공한 서비스 프로그램을 본인 단말기에 저장한다.
- [0067] 인증단계로, 모바일 쿠폰발행 해당 서비스에 가입한 회원(210)이, 자신의 온라인 또는 모바일 단말기인, 쿠폰발행 회원 단말기를 통해, 사전에 발급받은 인증코드 혹은 아이디와 암호 또는 개인 바코드 등을 쿠폰서비스 제공업체 서버(100)로 전송하면서 인증을 요청하고(S110), 쿠폰서비스 제공업체 서버(100)는 인증을 행하고(S120), 쿠폰발행 회원 단말기로 승인신호를 전송한다(S130).
- [0068] 수령자 설정단계로, 쿠폰발행 회원 단말기에서, 쿠폰을 발행하기 위해, 수령자를 설정한다(S140).

- [0069] 조건입력단계로, 쿠폰발행 회원 단말기에서, 특정활동의 목표를 설정한다(S145).
- [0070] 리워드 설정단계로, 쿠폰발행 회원 단말기에서, 리워드를 설정한다(S150).
- [0071] 결제단계로, 설정된 리워드에 대한 결제를 행한다(S155).
- [0072] 쿠폰발행 단계로, 쿠폰발행 회원 단말기에서, 쿠폰서비스 제공업체 서버(100)로 쿠폰 발행을 요청하고(S160), 쿠폰서비스 제공업체 서버(100)는 쿠폰발행 회원 단말기에서 요청된 쿠폰발행 여부를 검증하여(S170), 쿠폰발행의 승인 신호를 전송하고(S180), 쿠폰관련정보를 저장하고(S190), 쿠폰을 발행한다(S200).
- [0073] 경우에 따라서는 쿠폰서비스 제공업체 서버(100)로 쿠폰 발행을 요청하고(S160), 쿠폰서비스 제공업체 서버(100)는 쿠폰발행 회원 단말기에서 요청된 쿠폰발행 여부를 검증하여(S170), 쿠폰발행의 승인 신호를 전송하는(S180) 것을 생략하고, 쿠폰발행 회원 단말기에서 쿠폰을 바로 발행할 수 있다.
- [0074] 쿠폰 수령단계로, 쿠폰서비스 제공업체 서버(100) 또는 쿠폰발행 회원 단말기에서 쿠폰수령 회원 단말기로 발행된 쿠폰이 전송되며, 동시에 쿠폰관련정보도 전송된다(S210). 여기서 발행하는 쿠폰은 포인트나 스탬프 등 적립식의 쿠폰일 수 있다.
- [0075] 목표수행 단계로, 쿠폰과 쿠폰관련정보를 수신한 쿠폰수령 회원은 쿠폰수령 회원 단말기를 통해 목표 수행을 행한다(S220).
- [0076] 보상수령단계로, 쿠폰서비스 제공업체 서버(100)로 리워드요청을 행하고(S230), 쿠폰서비스 제공업체 서버(100)는 쿠폰수령 회원 단말기에서 수신된 리워드 요청을 검증하여(S240), 보상을 쿠폰수령 회원 단말기로 제공한다(S250).
- [0077] 경우에 따라서, 쿠폰서비스 제공업체 서버(100)로 리워드요청을 행하고(S230), 쿠폰서비스 제공업체 서버(100)는 쿠폰수령 회원 단말기에서 수신된 리워드 요청을 검증하는(S240) 것을 생략하고, 쿠폰 발행 회원단말기 또는 쿠폰서비스 제공업체 서버(100)에서 바로 보상을 쿠폰수령 회원 단말기로 제공할 수 있다.
- [0078] 도 3에서는 결제단계에서 설정된 리워드에 대한 결제를 무조건 진행하고(S155), 추후 쿠폰수령 회원은 쿠폰수령 회원 단말기를 통해 목표 수행을 다하지 못하였을 경우에, 환불이 되지 않는다. 쿠폰발행 회원에게 구매한 리워드 그대로 환불이 된다. 이 경우는 구매한 리워드는 반드시 소진을 해야 하며, 환불 행위가 없다.
- [0079] 도 4은 본 발명의 다른 일 실시예에 의한 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법을 개략적으로 설명하는 흐름도이다.
- [0080] 도 3의 결제단계 대신에, 도 4에서는 가결제 단계를 가지며, 즉 도 4의 가결제 단계에서는 설정된 리워드에 대한 가결제를 행한다(S157).
- [0081] 또한, 도 4에서는 보상 수령 단계 중, 보상을 쿠폰수령 회원 단말기로 제공하는(S250) 것에 앞서서, 설정된 리워드에 대해 가결제 되었던 것(S157)을 자동 결제하는 결제 단계를 가진다.
- [0082] 만약 쿠폰과 쿠폰관련정보를 수신한 쿠폰수령 회원이 쿠폰수령 회원 단말기를 통해 목표 수행을 다하지 못하였을 경우(S260)에는 설정된 리워드에 대해 가결제 되었던 것(S157)을 자동 환불하며(S267), 환불 시에는 일정 수수료가 발생될 수 있다. 이 외에는 도 4의 퍼스널 마케팅 방법은 도 3의 퍼스널 마케팅 방법과 같다.
- [0083] 도 5는 본 발명의 또 다른 일 실시예에 의한 모바일 적립 쿠폰과 온라인 쇼핑을 이용한 퍼스널 마케팅 방법을 개략적으로 설명하는 흐름도이다.
- [0084] 도 5에서는 쿠폰과 쿠폰관련정보를 수신한 쿠폰수령 회원이 쿠폰수령 회원 단말기를 통해 목표 수행을 다하지 못하였을 경우(S260)에는 설정된 리워드에 대해 결제되었던 것(S155)을 자동 환불한다(S267). 이 외에는 도 5의 퍼스널 마케팅 방법은 도 3의 퍼스널 마케팅 방법과 같다. 환불 시에는 일정 수수료가 발생될 수 있다.
- [0085] 즉, 도 3의 경우는 설정된 리워드에 대해 결제되면(S155), 쿠폰수령 회원의 목표 수행 여부와 상관없이 구매한 리워드는 환불이 되지 않는 반면, 도 5의 경우는 설정된 리워드에 대해 결제된후(S155), 쿠폰수령 회원의 목표 불수행시에는 구매한 리워드가 환불이 된다(S267).
- [0086] 다시 정리하면, 본 발명의 서비스는 모바일 기기를 통한 쿠폰발행, 이를 온라인 쇼핑과 연계하여 적립쿠폰의 리워드를 직접 선택하는 방법으로, 모바일 적립쿠폰은 이용자가 일정 목표치에 도달하면 해당 쿠폰이 자동적으로 사전에 쿠폰 발행자가 정한 리워드 상품 혹은 상품과 교환할 수 있는 상품권으로 변경되는 데, 이를 정리하면

다음과 같다.

- [0087] 첫째, 모바일 쿠폰 발행 서비스에 대해서 정리하면, 모바일 쿠폰발행 해당 서비스에 가입한 유저가 온라인 및 모바일 기기를 통해 사전에 발급받은 인증코드 혹은 아이디와 암호 또는 개인 바코드 등을 통해 제 3자에게 모바일 쿠폰발행이 가능하다. 발행하는 쿠폰은 포인트나 스탬프 등 적립식의 쿠폰이며 해당 쿠폰 발행 시 일정 목표치를 정한 후 해당 쿠폰의 목표치에 도달하면 제공하는 리워드를 서비스에서 제공하는 쇼핑몰 혹은 연계한 쇼핑몰에서 상품이나 상품권을 선택하여 지정한다. 지정한 상품이나 상품권은 쿠폰을 발급받은 유저가 목표치를 완료하면 자동적으로 변경하거나 구매가 된다. (미션완료)
- [0088] 둘째, 보상(리워드)에 대해서 정리하면, 본 발명에서 보상(리워드) 해당 서비스에서의 리워드란 결제가 필요한 실물이나 온라인 상품, 쿠폰, 상품권, 스탬프 등을 포함한다. 쿠폰을 발급하는 유저는 쿠폰 발행 시 보상 상품을 발행 단계에서 결제를 해야 한다. 결제는 반드시 금액이 지불되는 행위는 아니나 결제단계는 포함한다. 여기서 말하는 온라인 상품이란 온라인에서 사용할 수 있는 실물을 말하며 상품권은 온라인서비스에서 사용할 수 있는 쿠폰이나 상품권, 혹은 오프라인에서 결제 시 사용할 수 있는 실물교환 상품권도 포함한다. 보상에서의 쿠폰이란 각종 할인 쿠폰 및 이벤트 쿠폰 등을 말한다. 보상에서의 스탬프란 말 그대로 스탬프를 의미한다.
- [0089] 예를 들어 A라는 사람이 A' 라는 쿠폰을 발행하면서 쿠폰 리워드로 홍대 주변에서 인기 있는 B라는 카페의 스탬프 4개를 구매하여 선정한다.
- [0090] C라는 유저가 A' 라는 쿠폰을 발급받고 목표치를 완료했을 경우 C라는 유저가 B라는 카페의 스탬프 쿠폰B' 을 해당 서비스 내에서 소지하고 있다면 스탬프 쿠폰 B' 에서 스탬프 4개가 추가되고, 스탬프 쿠폰 B' 가 없다면 4개가 찍혀진 스탬프 쿠폰B' 을 받게 된다. 이 유저의 경우 스탬프 쿠폰B' 가 8개를 다 찍었을 때 아메리카노 1잔을 리워드로 받게 되어 있다면, 4개만 스탬프를 더 찍으면 아메리카노를 나실 수 있게 된다. 스탬프 쿠폰 B는 B라는 카페에서 제공하는 모바일 스탬프 쿠폰이며 해당 쿠폰은 해당 서비스 내에서 제공하고 있거나 타 모바일 쿠폰 서비스에서 제공하는 쿠폰일 수 있으며 후자의 경우 서비스 연계를 한 경우이다.
- [0091] 본 발명에서의 결제는 3가지 경우가 있을 수 있다. 가 결제 후 유저가 해당 기간 내 목표치를 완수하면 결제가 되고 목표치를 완료하지 못하면 도로 환불이 되는 경우, 처음부터 무조건 결제가 되고 유저가 해당 기간 내 목표치를 완료하지 못하면 환불이 되는 경우이며 환불 시에는 일정 수수료가 발생될 수 있다. 다른 또 하나는 무조건 결제가 진행되고 환불이 되지 않는 경우이며 구매한 리워드는 반드시 소진을 해야 한다. 환불 행위가 없을 수도 있다.
- [0092] 여기서, 무조건 결제가 진행되고 환불이 되지 않는 경우에, 구매한 리워드는, 리워드를 구매한 회원에게 남아 있을 경우, 그 회원은 자신의 디바이스(쿠폰발행 회원 단말기)에서 관련 정보를 확인할 수 있고 혹은 웹사이트 등 온라인에서 개인정보 로그인 후 확인할 수도 있으며, 남아 있는 리워드는 그대로 다른 쿠폰 발행을 할 때 이용할 수 있다. 즉 리워드가 있는 경우에는 결제 단계에서 사용할 수 있는 리워드 목록을 보여주고 선택을 할 수 있게 한다.
- [0093] 셋째, 모바일 쿠폰 수령에 대해 정리하면, 모바일 쿠폰 수령 해당 서비스에 가입 후 해당 서비스를 이용하는 유저에게서 쿠폰을 발급받을 수 있다. 쿠폰을 수령한 유저는 해당 쿠폰에서 제시한 기간 내에 목표치에 도달하면 해당 적립쿠폰은 자동적으로 정해진 온라인 상품권이나 포인트, 실물 등 리워드를 수령할 수 있다. 좀 더 쉽게 말하면 적립 쿠폰이 자동적으로 리워드로 변경되는 것이다.
- [0094] 넷째, 본 발명을 이용한 서비스활용에 대해 설명하면, 서비스의 활용 1인 기업과 부모와 자식간의 관계 등에서 교육적인 목표 등으로 사용할 수 있다.
- [0095] 예를 들어 초등학교 1학년인 자녀를 둔 학부모가 아이의 교육차원에서 모바일 스탬프 쿠폰을 발행한다. 쿠폰의 유효기간은 한 달이며 해당 기간 내에 심부름을 열 번하면 온라인 문화상품권 5,000원을 지급한다. 해당 자녀가 열 번의 심부름을 하게 되면 해당 모바일 적립쿠폰은 자동적으로 온라인 문화상품권으로 변경된다.
- [0096] 다른 예로서, 보험설계사인 A씨는 많은 고객을 만나고 대접해야 하는 업무의 특성상 자신이 관리하는 100명의 고객들에게 쿠폰을 발행한다. 만날 때마다 스탬프 1개, 고객 추천 시 스탬프 5개로 규칙을 정하고 스탬프 10개가 채워지면 XX 커피전문점의 아메리카노 기프트권이 해당 고객에게 전송된다.
- [0097] 또한, 본 발명에서 서비스의 활용 스탬프를 리워드로 활용한 새로운 마케팅으로의 활용도 가능하다. 예를 들어 A라는 카페가 자신들의 스탬프 쿠폰에서 찍어주는 스탬프를 B라는 보험설계사 C에게 저렴한 가격으로 스탬프를 제공함으로써 A라는 카페는 고객층 확대가 가능하고 보험설계사 C는 저렴한 비용으로 퍼스널 마케팅이

가능하다.

- [0098] 다섯째, 서비스의 구조에 대해서 설명하던, 본 발명의 서비스의 실행은 스마트폰을 포함하여 앱을 실행할 수 있는 모든 모바일 기기, 온라인을 포함한다.
- [0099] 회원은 서비스 프로그램을 통하여 가입을 하여야 하며, 가입은 간단한 가입단계로 이루어진다.
- [0100] 쿠폰 수령자 선택에 있어서, 쿠폰을 발행하는 회원의 단말기(디바이스)에서 수령자 선택이 가능하며, 경우에 따라서 수령자의 단말기에서 직접 쿠폰 발행도 가능하다. 수령자의 단말기에서 직접 발행 시 별도의 수령자 선택 단계는 필요 없다. 온라인도 가능하다.
- [0101] 리워드 선택에 있어서 보상은 온라인 쇼핑물에서 쇼핑을 하듯 해당 서비스 내 연계된 혹은 속해있는 쇼핑물에서 상품을 쇼핑하여 설정한다. 즉, 리워드 선택은, 서비스 프로그램 내에 고정된 다수개의 상품도 가능하고 실제 기존 온라인 쇼핑물에서 상품을 선택할 수도 있다. 기존 온라인 쇼핑물에서 상품을 선택하는 경우 해당 서비스와의 연계를 통해 진행한다.
- [0102] 여기서, 서비스 내 연계된 혹은 속해있는 쇼핑물이란, 즉, 쿠폰제공업체에서 자체적으로 쇼핑물을 제작하여 서비스 내 혹은 프로그램 내 서비스 하는 경우 (직접 서비스)인, 서비스 내 쇼핑물과, 기존에 구축되어 있는 온라인 쇼핑물을 서비스 혹은 프로그램 내에 연동시켜 위탁서비스를 하는 경우인, 연계된 쇼핑물을 포함한다.
- [0103] 도 6은 본 발명의 일실시예에 의한 리워드 결제 및 전달을 설명하기 위한 흐름도이다. 도 6은 쿠폰 제공업체 자체에서 리워드 제공하는 경우이다.
- [0104] 리워드 설정단계로, 발행자는 쿠폰발행 회원단말기에서 온라인 쇼핑물 등을 통해 리워드설정한다(S150).
- [0105] 결제요청 단계로, 쿠폰발행 회원단말기에서 쿠폰서비스 제공업체, 즉, 쿠폰서비스 제공업체 서버로 결제정보의 전송과 함께 결제요청을 하며(S151-1), 쿠폰서비스 제공업체는 쿠폰발행 회원단말기에서 수신된 결제정보를 결제대행업체, 즉, 결제대행업체 서버로 전송함과 함께, 결제대행업체 서버로 결제요청을 행한다(S151-2).
- [0106] 승인단계로, 결제대행업체 서버는 발행자의 쿠폰발행 회원단말기로 결제에 따른 승인요청을 행하고(S152-1), 발행자는 쿠폰발행 회원단말기를 통해 승인을 행하고, 그 승인결과는 결제대행업체 서버로 전송된다(S152-2).
- [0107] 결제단계로, 승인단계에서 승인된 후, 결제대행업체 서버는 결제를 행하여 결제를 완료하고(S154), 결제대행업체 서버는 결제정보(즉, 결제된 정보)를 쿠폰서비스 제공업체 서버로 전송하고(S156-1), 쿠폰서비스 제공업체 서버는 수신된 결제정보를 발행자의 쿠폰발행 회원단말기로 전송하여 결제정보를 확인하게 한다(S156-2).
- [0108] 대금지급단계로, 결제대행업체는 쿠폰서비스 제공업체로 대금을 지급하고(S157-1), 쿠폰서비스 제공업체는 결제대행업체로부터 대금을 수신한다(S157-2).
- [0109] 다음은 쿠폰서비스 제공업체서버에서 쿠폰이 발행되어 수신자에게 전송된 후 목표수행에 따라 리워드(즉, 상품/상품권)를 제공하는 흐름을 설명한다.
- [0110] 목표수행 단계로, 쿠폰을 수신한 쿠폰수령 회원은 쿠폰수령 회원 단말기를 통해 목표 수행을 행한다(S220).
- [0111] 정보수신단계로, 목표수행 단계에서 수신자가 목표 수행을 완료하면, 목표 수행을 완료하였다는 정보를 쿠폰수령 회원단말기를 통해 쿠폰서비스 제공업체 서버로 전송한다(S232).
- [0112] 보상수령단계로, 쿠폰서비스 제공업체 서버는 상품/상품권으로 이루어진 리워드(보상)을 수신자에게 전달되어 (S247), 수신자는 상품/상품권으로 이루어진 리워드(보상)를 수령한다(S250).
- [0113] 도 7은 본 발명의 다른 일실시예에 의한 리워드 결제 및 전달을 설명하기 위한 흐름도이다. 도 7은 외부쇼핑업체에서 리워드를 제공하는 경우이다.
- [0114] 도 7의 리워드 설정단계(S150) 내지 결제단계(S154, S156-1, S156-2)은 도 6의 그것과 동일하다. 따라서 이에 대한 설명은 생략한다.
- [0115] 결제단계(S154, S156-1, S156-2) 후의 대금지급단계는 다음과 같다.
- [0116] 대금지급단계로, 결제대행업체는 쿠폰서비스 제공업체 또는 (외부)쇼핑업체로 대금을 지급하고(S157-1), 쿠폰서비스 제공업체 또는 (외부)쇼핑업체는 결제대행업체로부터 대금을 수신한다(S157-2).
- [0117] 다음은 쿠폰서비스 제공업체서버에서 쿠폰이 발행되어 수신자에게 전송된 후 목표수행에 따라 리워드(즉, 교환



권/상품)를 제공하는 흐름을 설명한다.

- [0118] 쿠폰서비스 제공업체로 상품 교환권전달 단계로, (외부)쇼핑업체는 리워드인 상품으로 교환할 수 있는 상품 교환권을 쿠폰서비스 제공업체로 전달하며(S212), 쿠폰서비스 제공업체는 상품 교환권을 수신한다(S214).
- [0119] 목표수행 단계로, 쿠폰을 수신한 쿠폰수령 회원(수신자)은 쿠폰수령 회원 단말기를 통해 목표 수행을 행한다(S220).
- [0120] 정보수신단계로, 목표수행 단계에서 수신자가 목표 수행을 완료하면, 목표 수행을 완료하였다는 정보를 쿠폰수령 회원단말기를 통해 쿠폰서비스 제공업체 서버로 전송한다(S232).
- [0121] 쿠폰수령 회원에게로 상품 교환권전달 단계로, 쿠폰서비스 제공업체 서버는 상품 교환권을 쿠폰수령 회원(수신자)에게 전달하여(S243), 쿠폰수령 회원(수신자)은 상품 교환권을 수신한다(S244).
- [0122] 쿠폰수령 회원이 상품수령 단계로, 쿠폰수령 회원(수신자)은 상품교환 또는 신청을 행하며(S246), 이에 따라 (외부)쇼핑업체는 상품을 전달하여(S247), 결과적으로 쿠폰수령 회원(수신자)가 상품을 수령한다.
- [0123] 도 8은 본 발명에서 쿠폰발행 회원 단말기를 통해 쿠폰을 발행하는 경우를 설명하는 설명도이다.
- [0124] 쿠폰발행 회원(발행자)은 쿠폰발행 회원 단말기(발행자의 단말기)로 온라인접속을 하여, 수령자를 선택하고(S140), 쿠폰을 발행한다(S200).
- [0125] 쿠폰서비스 제공업체 서버는 쿠폰관련정보를 쿠폰발행 회원 단말기로부터 수신하고, 쿠폰 및 쿠폰관련 정보를 수령자 단말기로 전달한다.
- [0126] 수령자는 수령자 단말기를 통해 쿠폰서비스 제공업체 서버로부터 전송되는 쿠폰 및 쿠폰관련 정보를 수신한다(212). 이렇게 하여, 수령자 단말기에 쿠폰이 생성된다.
- [0127] 여기서, 온라인이라 함은 웹사이트나 프로그램 실행을 통해 접속을 하는 형태며 인터넷 접속이 되는 환경을 말한다. 또한, 수령자 단말기상의 쿠폰생성은 수령자 단말기에 설치된 프로그램을 통해 실행된다.
- [0128] 도 9는 본 발명에서 수령자 단말기에서 쿠폰을 발행하는 경우를 설명하는 설명도이다. 이는 발행자가 수령자 단말기를 이용하여 쿠폰을 발행하는 경우이다.
- [0129] 우선 수령자 단말기에 쿠폰서비스 제공업체에서 배포한 프로그램(서비스)을 실행시키고, 수령자 단말기를 사용하여 발행자(쿠폰발행 회원)를 설정하고, 선택버튼(또는 선택키) 중 쿠폰발행을 선택한다.
- [0130] 다음에 수령자 단말기를 통해 발행자 인증을 행하며(S120), 인증시, 쿠폰서비스 제공업체 서버로 인증에 필요한 정보를 전송하게 되며, 쿠폰서비스 제공업체 서버는 이를 수신하게 된다. 즉, 사전에 발행자가 발급받은 인증코드 혹은 아이디와 암호 또는 개인 바코드 등을 쿠폰서비스 제공업체 서버(100)로 전송하면서 인증을 요청하고, 쿠폰서비스 제공업체 서버는 이를 인증을 행하고, 수령자 단말기로 승인신호를 전송한다.
- [0131] 다음에 발행자는 수령자 단말기를 통해 특정활동의 목표를 설정하고, 디워드를 설정하고 설정된 디워드에 대한 결제를 행하고, 수령자 단말기에서, 쿠폰서비스 제공업체 서버로 쿠폰 발행을 요청하고, 쿠폰서비스 제공업체 서버는 수령자 단말기에서 요청된 쿠폰발행 여부를 검증하여 쿠폰발행의 승인 신호를 수령자 단말기로 전송하여, 수령자 단말기에 쿠폰이 생성된다. 또한, 쿠폰서비스 제공업체 서버는 자체적으로 쿠폰관련정보를 저장하며, 동시에 쿠폰관련정보 등을 발행자 단말기로 전송한다.
- [0132] 본 발명에서 수령자 단말기에서 직접 쿠폰 발행 시 발행자 인증방법에는 크게 2가지가 있다. 첫 번째 방법은 기존의 온라인 서비스처럼 회원가입 후 별도의 인증코드 혹은 식별코드를 부여 받는 경우(일종의 아이디)이고, 두 번째는 모바일 인증기를 통한 발행자 인증방법으로, 모바일 인증기는 일종의 모바일 otp방식으로 해당 otp를 모바일 앱 혹은 프로그램으로 구현 후 실행하여 인증코드를 입력하는 방식이다
- [0133] 도 10은 본 발명에서 수령자 단말기에서 직접 쿠폰 발행 시 발행자 인증방법의 일실시예의 흐름도이다. 도 10은 기존의 온라인 서비스처럼 회원가입 후 별도의 인증코드 혹은 식별코드(일종의 아이디)를 부여 받는 경우이다.
- [0134] 도 10은 도 9와 같이 수령자 단말기에서 쿠폰을 발행하는 경우로, 여기서 사용하는 인증을 위해, 사전에 발행자는 쿠폰서비스 제공업체에 회원가입하되, 회원가입에 필요한 정보를 쿠폰서비스 제공업체에 전송하고, 쿠폰서비스 제공업체는 이를 수신한 후, 인증코드를 부여하여 발행자에게 전송하고, 발행자는 인증코드를 수신한다.
- [0135] 그 다음에, 도 9와 같이, 발행자는 수령자 단말기에 쿠폰서비스 제공업체에서 배포한 프로그램(서비스)을 실행

시키고, 수령자 단말기를 사용하여 발행자(쿠폰발행 회원)를 설정하고, 선택버튼(또는 선택키) 중 쿠폰발행을 선택한다.

- [0136] 그리고 수령자 단말기를 통해 발행자 인증을 행하며, 인증시, 인증코드를 입력하여, 쿠폰서비스 제공업체 서버로 인증코드를 전송하게 되며, 쿠폰서비스 제공업체 서버는 이를 수신하게 된다. 쿠폰서비스 제공업체 서버는 이를 이용하여 인증을 행하고, 수령자 단말기로 승인신호를 전송한다.
- [0137] 다음에 발행자는 수령자 단말기를 통해 특정활동의 목표를 설정하고, 리워드를 설정하고 설정된 리워드에 대한 결제를 행하고, 수령자 단말기에서, 쿠폰서비스 제공업체 서버로 쿠폰 발행을 요청하고, 쿠폰서비스 제공업체 서버는 수령자 단말기에서 요청된 쿠폰발행 여부를 검증하여 쿠폰발행의 승인 신호를 수령자 단말기로 전송하여, 수령자 단말기에 쿠폰이 생성된다. 또한, 쿠폰서비스 제공업체 서버는 자체적으로 쿠폰관련정보를 저장하며, 동시에 쿠폰관련정보 등을 발행자 단말기로 전송하여, 고객 DB를 생성관리한다.
- [0138] 도 11은 본 발명에서 수령자 단말기에서 직접 쿠폰 발행 시 발행자 인증방법의 다른 실시예의 흐름도이다. 도 11은 모바일 인증기를 통한 발행자 인증방법이다.
- [0139] 도 11에서는, 쿠폰서비스 제공업체에서 제공한 모바일 디바이스용 프로그램인, 모바일 인증기를 다운로드하여, 실행시키고, 식별코드를 확인하고, 식별코드를 등록하고, 쿠폰서비스 제공업체 서버에 이를 전송하고, 쿠폰서비스 제공업체 서버는 이를 수신하여 저장관리한다.
- [0140] 그 다음에, 도 9와 같이, 발행자는 수령자 단말기에 쿠폰서비스 제공업체에서 배포한 프로그램(서비스)을 실행시키고, 수령자 단말기를 사용하여 발행자(쿠폰발행 회원)를 설정하고, 선택버튼(또는 선택키) 중 쿠폰발행을 선택한다.
- [0141] 그리고 수령자 단말기를 통해 발행자 인증을 행하며, 인증시, 식별코드(즉, 인증코드)를 입력하여, 쿠폰서비스 제공업체 서버로 식별코드(인증코드)를 전송하게 되며, 쿠폰서비스 제공업체 서버는 수령자 단말기로부터 식별코드(인증코드)를 수신하고, 또한 모바일 인증기를 실행하여 인증코드를 수신하여 인증을 행하고, 수령자 단말기로 승인신호를 전송한다.
- [0142] 다음에 발행자는 수령자 단말기를 통해 특정활동의 목표를 설정하고, 리워드를 설정하고 설정된 리워드에 대한 결제를 행하고, 수령자 단말기에서, 쿠폰서비스 제공업체 서버로 쿠폰 발행을 요청하고, 쿠폰서비스 제공업체 서버는 수령자 단말기에서 요청된 쿠폰발행 여부를 검증하여 쿠폰발행의 승인 신호를 수령자 단말기로 전송하여, 수령자 단말기에 쿠폰이 생성된다.
- [0143] 도 12는 본 발명의 퍼스널 마케팅 시스템에서 수령자 단말기를 이용하여 쿠폰 발행시의 일예이다.
- [0144] 도 12는 발행자가 직접 쿠폰 수령자 단말기에서 쿠폰생성을 하는 경우의 실행화면의 예를 나타낸다. 이 경우는 해당 화면에 사전에 발행정보가 미리 저장되어 있는 경우이다.
- [0145] 도 12의 (a)는 쿠폰서비스 제공업체 서버로 쿠폰 발행을 요청하기 위해, 쿠폰발행 선택키를 선택하는 화면을 나타내며, 도 12의 (b)는 인증을 위해 인증코드를 입력하기위한 화면을 나타내며, 도 12의 (c)는 쿠폰이 발행되었을 때의 화면을 나타내며, 도 12의 (d)는 수령자 단말기에 쿠폰이 생성된 화면을 나타낸다.
- [0146] 도 13은 본 발명의 퍼스널 마케팅 시스템에서 수령자 단말기를 이용하여 쿠폰 발행시의 다른 일예이다. 이 경우는 직접적으로 발행정보를 입력하는 경우로, 사전에 발행정보가 저장되어 있지 않은 경우이다.
- [0147] 도 13의 (a)는 인증을 위해 인증코드를 입력하기위한 화면을 나타내며, 도 13의 (b)는 수령자 단말기를 통해 특정활동의 목표, 즉 미션타입, 목표개수, 유효기간 등을 설정하는 화면이다.
- [0148] 도 13의 (c)는 리워드를 설정하는 화면으로, 도 13의 (c)의 화면에서 리워드는 여러 개 구매가 가능하며 남은 리워드는 저장되어 다음 쿠폰 발행 때 쇼핑에서 선택할 수 있다. 도 13의 (b)~(c)는 사전에 고정하여 등록하고, 다음 번의 쿠폰 발행 때는 해당 단계는 건너뛰게 할 수 있다.
- [0149] 도 13의 (d)는 설정된 리워드에 대해 결제를 행하는 화면이다.
- [0150] 도 14는 본 발명의 퍼스널 마케팅 시스템에서 쿠폰의 생성 및 리워드 수신을 나타내는 화면들의 예이다.
- [0151] 도 14의 (a)는 수령자 단말기에 쿠폰이 수신된 화면을 나타내며, 도 14의 (b)는 수령자가 목표 수행을 완료하여 리워드(보상)로서 상품권이 수신된 화면을 나타낸다. 도 14의 (b)는 해당 쿠폰이 소정 개수를 도달해야 한다는 목표(미션)을 완료하여, 도 14의 (a)의 스탬프 쿠폰이 온라인 상품권으로 바뀐 것을 나타낸다. 도 14의 (a)의

스탬프 쿠폰은 목표(미션) 완료 시 자동으로 삭제된다.

[0152] 도 14의 (c)는 수령자가 목표 수행을 완료하여 리워드(보상)로서 스탬프가 지급된 화면을 나타내며, 도 14의 (d)는 도 14의 (c)의 '확인하기' 버튼을 눌러 스탬프가 적립된 상태를 나타내는 화면이다.

[0153] 즉, 도 14의 (b)의 화면은 일반 (온라인) 상품권을 보상으로 지급한 경우, 도 14의 (c)의 화면은 같은 서비스 내 다른 쿠폰의 스탬프를 보상으로 지급한 경우이다.

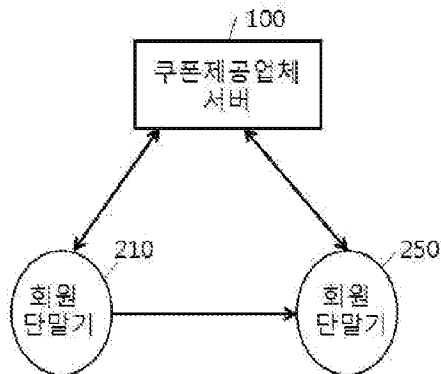
[0154] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 이는 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명의 사상은 아래에 기재된 특허청구범위에 의해서만 파악되어야 하고, 이의 균등 또는 등가적 변형 모두는 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

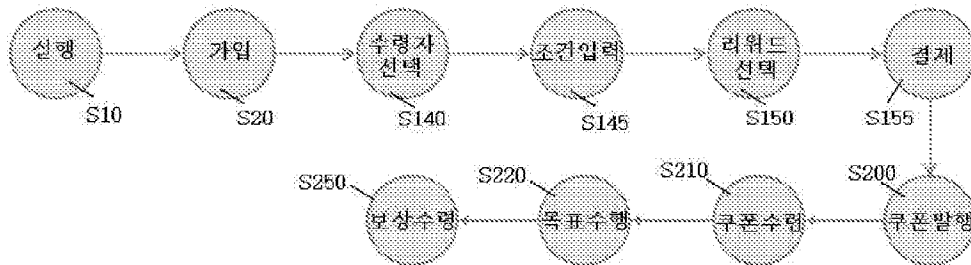
[0155] 100: 쿠폰제공업체 서버  
210, 250: 회원 단말기

도면

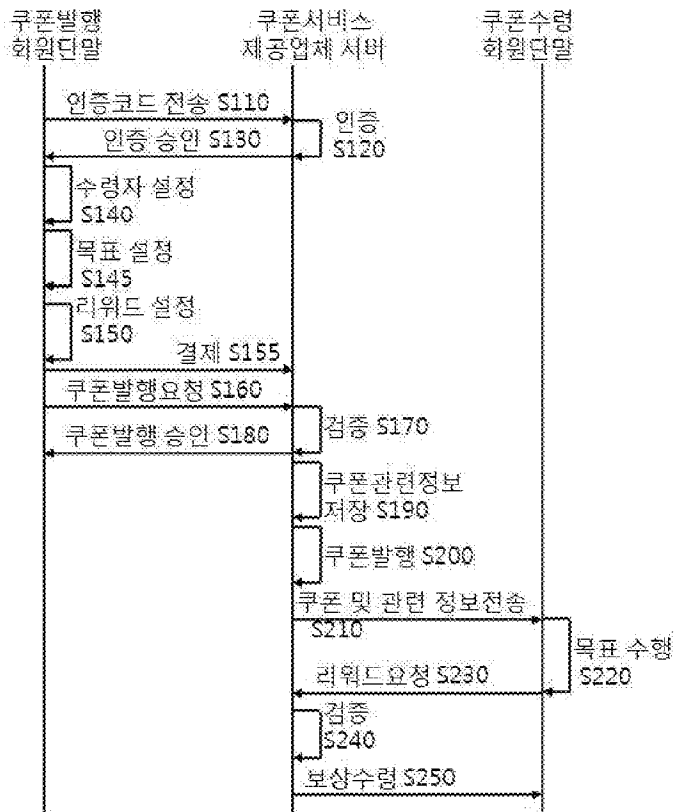
도면1



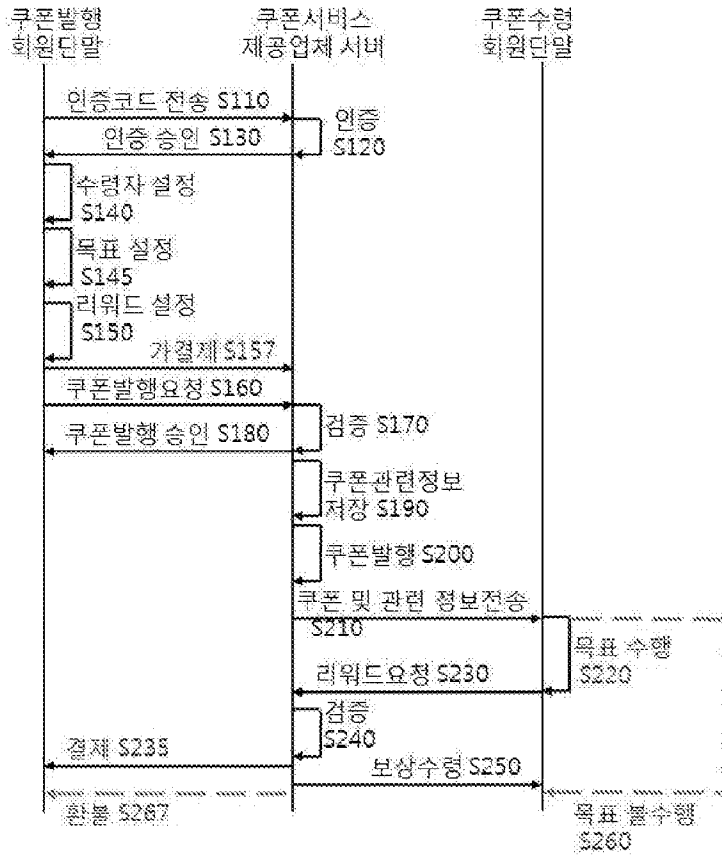
도면2



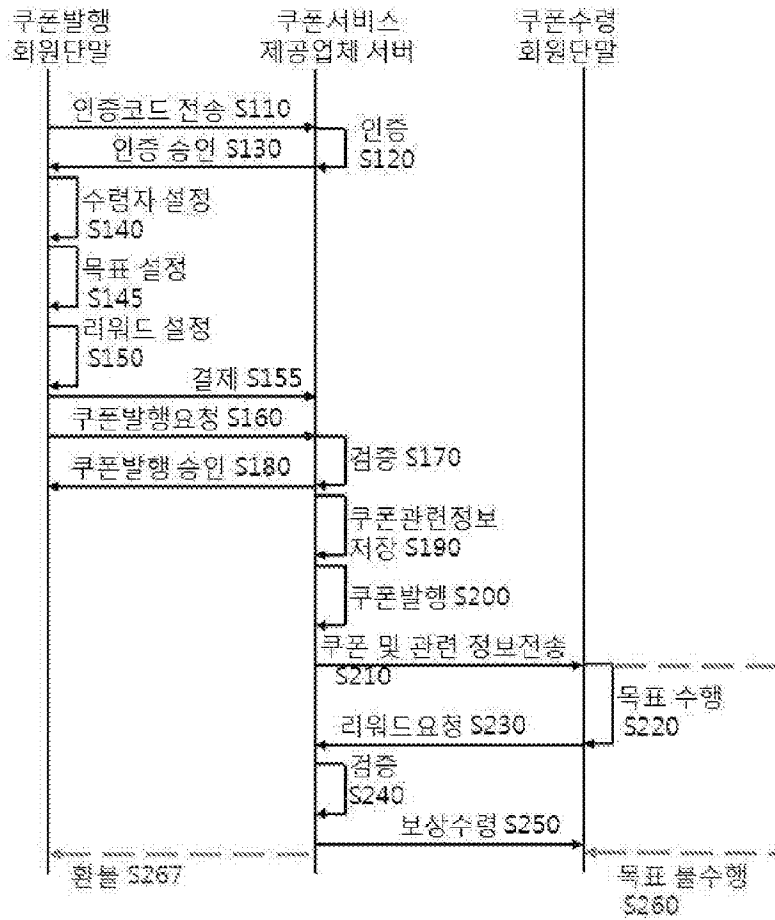
도면3



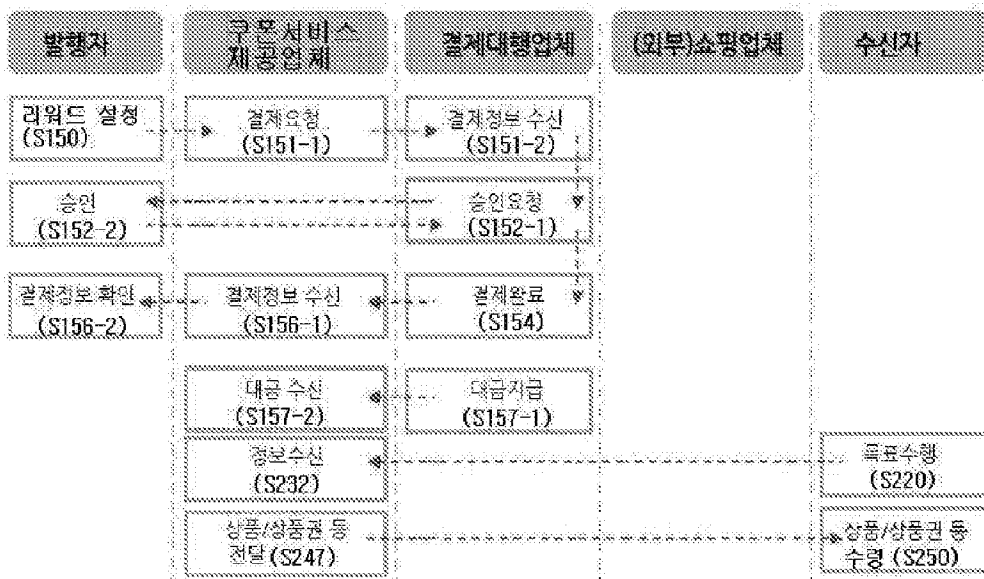
도면4



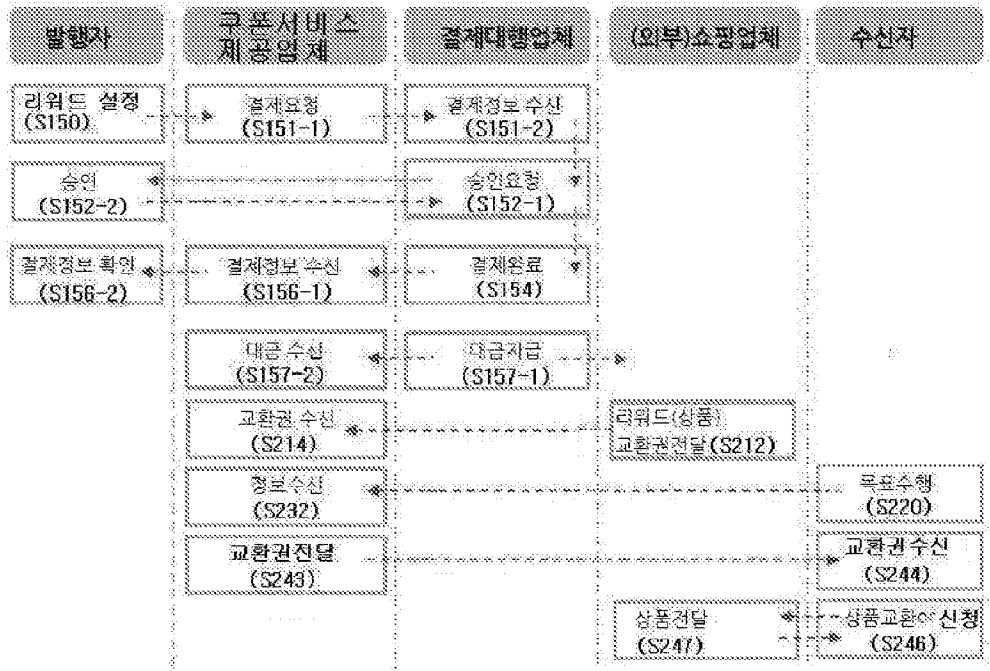
도면5



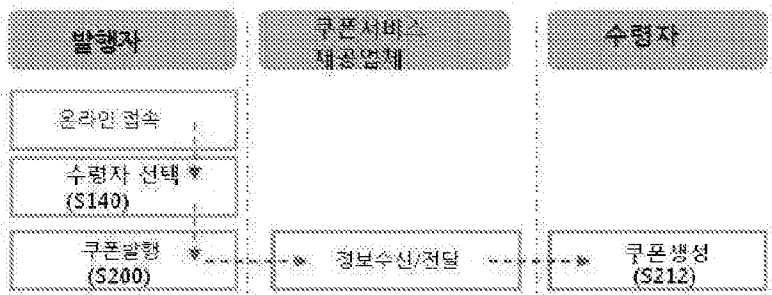
도면6



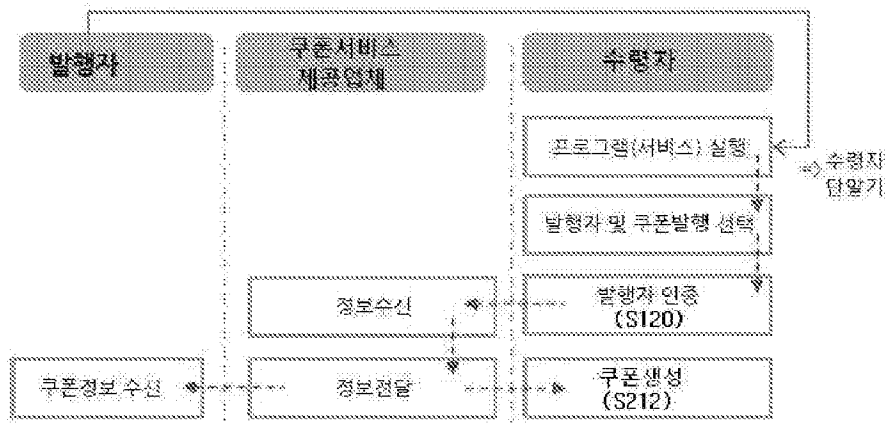
도면7



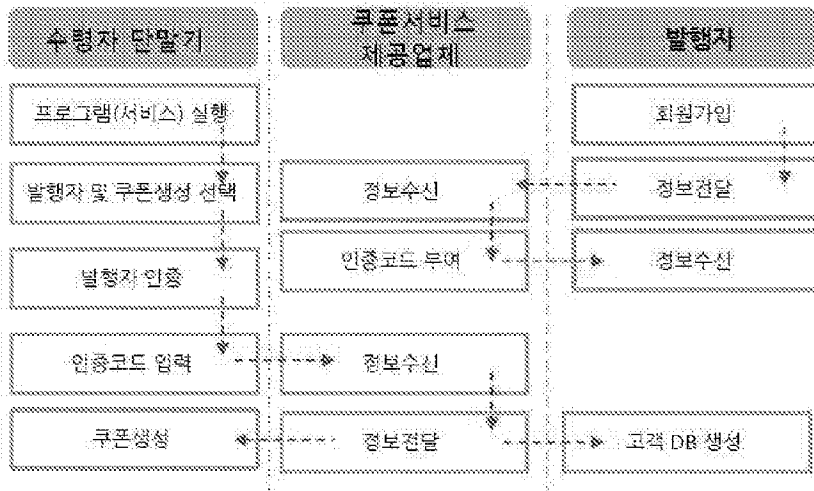
도면8



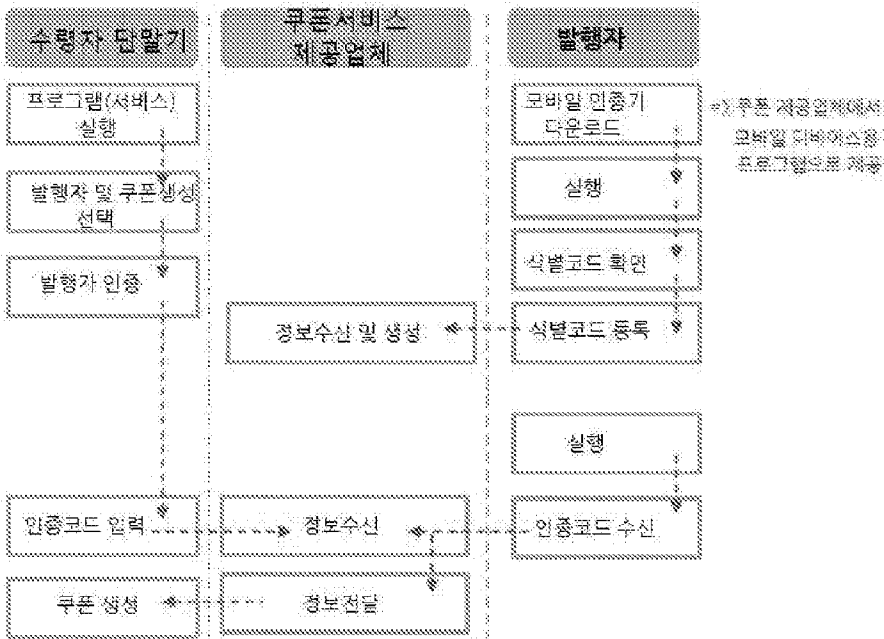
도면9



도면 10

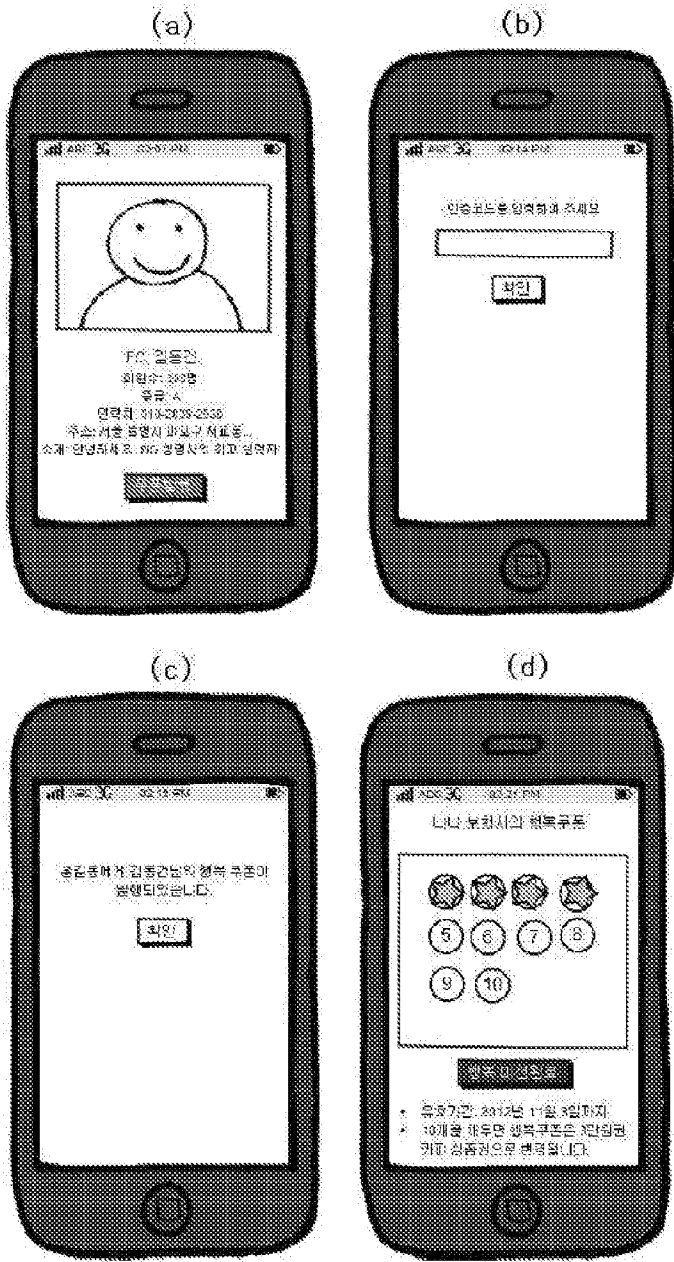


도면 11

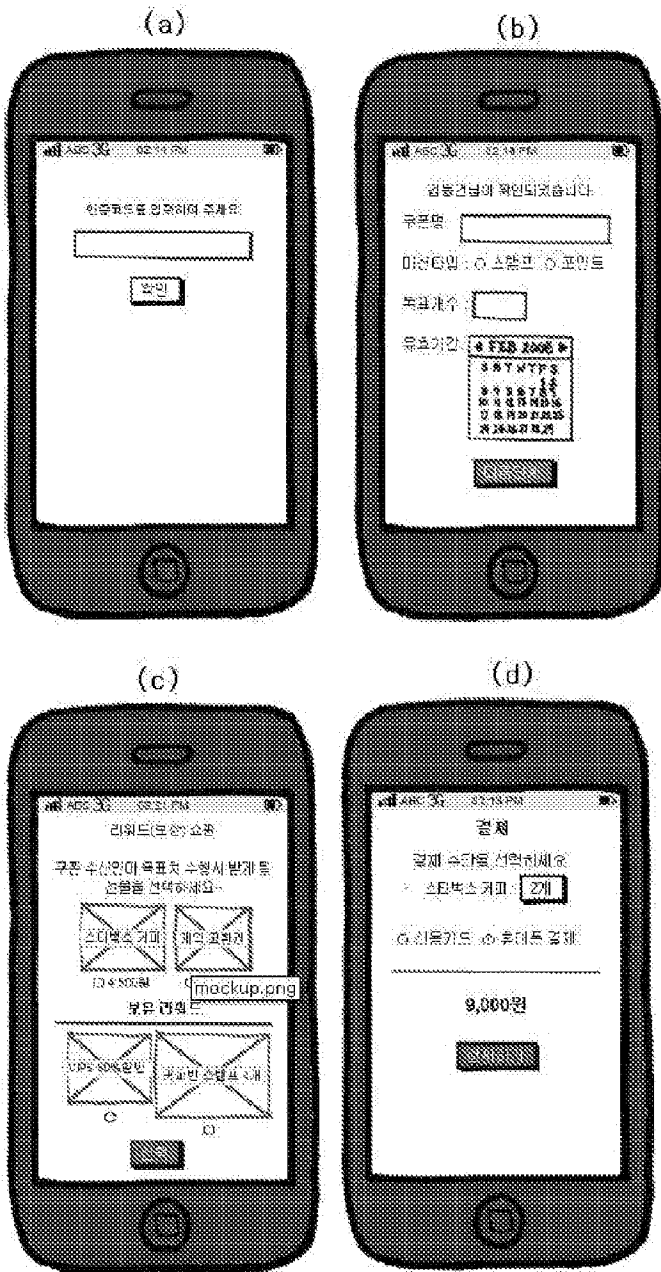




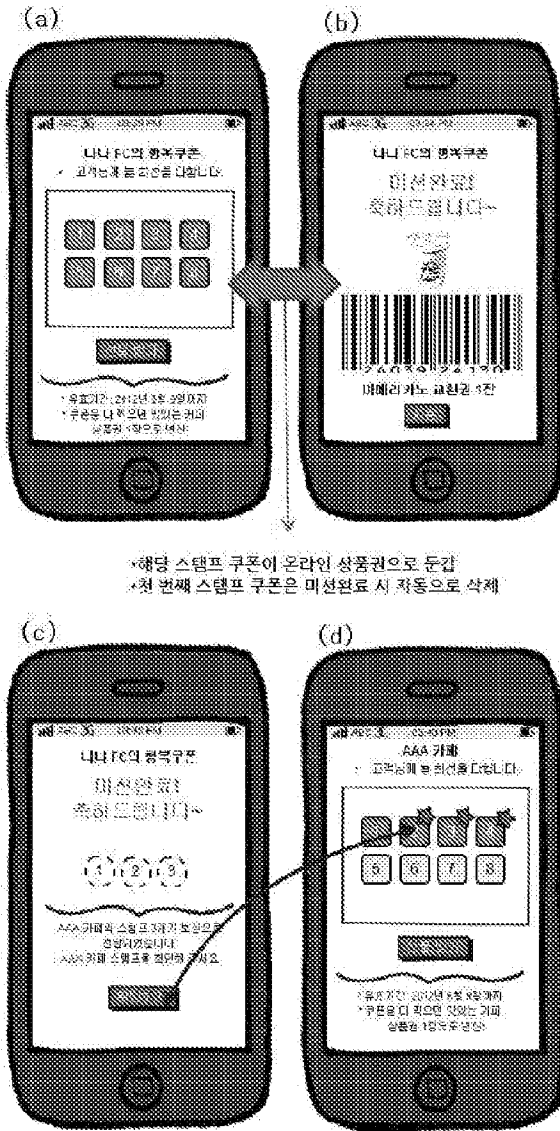
도면 12



도면 13



도면 14





UNITED STATES  
PATENT AND TRADEMARK OFFICE

P.O. Box 1450  
Alexandria, VA 22313 - 1450  
www.uspto.gov

## ELECTRONIC PAYMENT RECEIPT

APPLICATION #  
18/197,070

RECEIPT DATE / TIME  
12/19/2023 09:26:50 PM Z ET

ATTORNEY DOCKET #  
104402-5074-US

### Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

### Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5568	FILED BY	Jackeline De Ranieri
PATENT CENTER #	63679679	AUTHORIZED BY	Douglas Crisman
CUSTOMER #	24341	FILING DATE	05/14/2023
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Paresh K. Patel

### Payment Information

PAYMENT METHOD DA / 500310	PAYMENT TRANSACTION ID E2023BIL27498310	PAYMENT AUTHORIZED BY Jackeline De Ranieri
PRE-AUTHORIZED ACCOUNT 500310	PRE-AUTHORIZED CATEGORY 37 CFR 1.19 (Document supply fees); 37 CFR 1.21 (Miscellaneous fees and charges)	

FEE CODE	DESCRIPTION	ITEM PRICE(\$)	QUANTITY	ITEM TOTAL(\$)
2806	SUBMISSION OF AN INFORMATION DISCLOSURE STATEMENT	104.00	1	104.00
			<b>TOTAL AMOUNT:</b>	<b>\$104.00</b>

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d))

Petitioner Exhibit 1002-4162

and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

**National Stage of an International Application under 35 U.S.C. 371**

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

**New International Application Filed with the USPTO as a Receiving Office**

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/265078551>

# THE COMMODITY VENDING MACHINE

Article · February 2005

CITATION  
1

READS  
16,624

1 author:



Susanne Gruber

Association for Research in Commodity Science - Forschungsverein für Warenlehre und angewandte Naturwissenschaften

38 PUBLICATIONS 10 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



Quellung von Asphalt, Ursachen und Auswirkungen [View project](#)



Die Wiener Warenkundesammlung - Herkunft und Bedeutung [View project](#)

## THE COMMODITY VENDING MACHINE

*Susanne GRUBER, Renate BUBER, Bernhart RUSO, Johannes GADNER*

Univ.-Ass. Dr. Susanne Gruber, Institute of Technology and Sustainable Product Management, University of Economics and Business Administration Vienna, Augasse 2 - 6, A-1090 Vienna, Austria, susanne.gruber@wu-wien.ac.at

Ass. Prof. Dr. Renate Buber, Institute of Retailing and Marketing, University of Economics and Business Administration Vienna, Augasse 2 - 6, A-1090 Vienna, Austria, renae.buber@wu-wien.ac.at

Dr. Bernhart Ruso, Institute of Knowledge Organisation, Lange Gasse 63/15, A-1080 Wien, Austria, bernhart@ruso.at

Dr. Johannes Gadner, Institute of Knowledge Organisation, Lange Gasse 63/15, 1080 Vienna, Austria, johannes.gadner@iwo.at

### Abstract

This paper describes the groups of players in the vending market and introduces a typology of vending machines. From a commodity perspective, vending includes the discussion of the types of vending machines and their technical demands for storing and preparing goods and services and for installing the vending machine at a certain location. From a marketing perspective, vending is defined as the distribution and selling of goods and services by a vending machine. In addition, a vending machine is seen as a distribution channel of a retailer. In the vending market, four groups of players can be differentiated: (1) the producers of the vending machines and the accessories as well as the goods; or the service providers; (2) the site lessors; (3) the operators, merchandisers and maintenance people; and (4) the customers.

The different types of vending machines can be categorized into product-oriented and service-oriented machines. Product-oriented vending machines offer both cold and hot food as well as non-food items. Service-oriented vending machines offer different kinds of services, e.g. entertainment (jukeboxes, slot machines) and non-entertainment (telephones or scales). In addition, from packaging refund machines the customer can get the packaging deposit back.

**Keywords:** vending, vending machine, distribution, operator, site lessor

### Introduction

The first vending machine was constructed by Heron of Alexandria (Mechanicus, about 100 BC). After inserting a coin, holy water was dispensed.<sup>1</sup> For more than 100 years people have been able to buy goods and services from vending machines. The first commercial vending machines were built at the end of the 80's of the 19<sup>th</sup> century.<sup>2</sup> On 13 March 1908, the first stamp and postcard-vending machine of the world was installed in front of the Hotel des Postes.<sup>3</sup>

Vending machines are used in different markets, in the retail trade for the selling of food and non-food items as well as convenience products. Selling cold and hot drinks was the predominant business in the past, but at present, the variety of goods and services marketed with vending machines is steadily increasing. Vending Associations in different countries define vending differently.

Basically, vending is defined as the selling of products through vending machines<sup>4</sup>, which are "coin operated machines for the sale of small articles"<sup>5</sup>. Additionally, vending machines can be designed for the sale of large quantities of various products, e.g. in Japan, one can buy ten-kilo bags of rice from a vending machine<sup>6</sup>. Furthermore, for a couple of years, it has been possible to pay for goods and services by credit card which has to be put in the vending machine's slot for cards.

The American Association NAMA (National Automatic Merchandising Association) states that "vend is the delivery of a single unit of merchandise"<sup>7</sup>. In the US, vending is highly connected with the slogan "Coffee, Candy, Cola"<sup>8</sup>. "Coffee" symbolises the sale of hot drinks like coffee, hot chocolate, tea, but also soups; the term "Candy" represents sweets, and "Cola" replaces the enumeration of different soft drinks. In the very beginning, the vending industry started with the 4-Cs-concept, coffee, cup soda, candy and cigarettes, and later on the range grew to almost 8 Cs - coffee, candy or confections, chips, cold drinks, canned drinks, cigarettes, cold cup and commissary.<sup>9</sup>

In Europe vending includes a wider range of products (EVA, European Vending Association)<sup>10</sup>. The Vending Association in Germany (BDV, Bundesverband der Deutschen Vending Automaten-Wirtschaft e.V.) defines vending as the selling of everyday essentials, especially food and drinks through vending machines. Producers of machines, operators and different associations use the term vending for all kinds of food and drinks, but they include non-food products as well.

The Austrian Association (ÖVV, Österreichische Verkaufsautomaten Vereinigung) defines all machines that sell goods, including food, drinks, photos, parking-tickets as vending machines; but

copying-machines, telephones, lockers, washing-machines, pin balls, slot machines, etc. are also included.<sup>11</sup> The BDV excludes machines which offer amusement features from the vending industry.<sup>12</sup>

From a marketing point of view, vending machines are defined as a store format of the retail trade industry with an automatic selling procedure – the customer has to select the product, to take it with him/her and to pay for it, everything is done by him-/herself.<sup>13</sup>

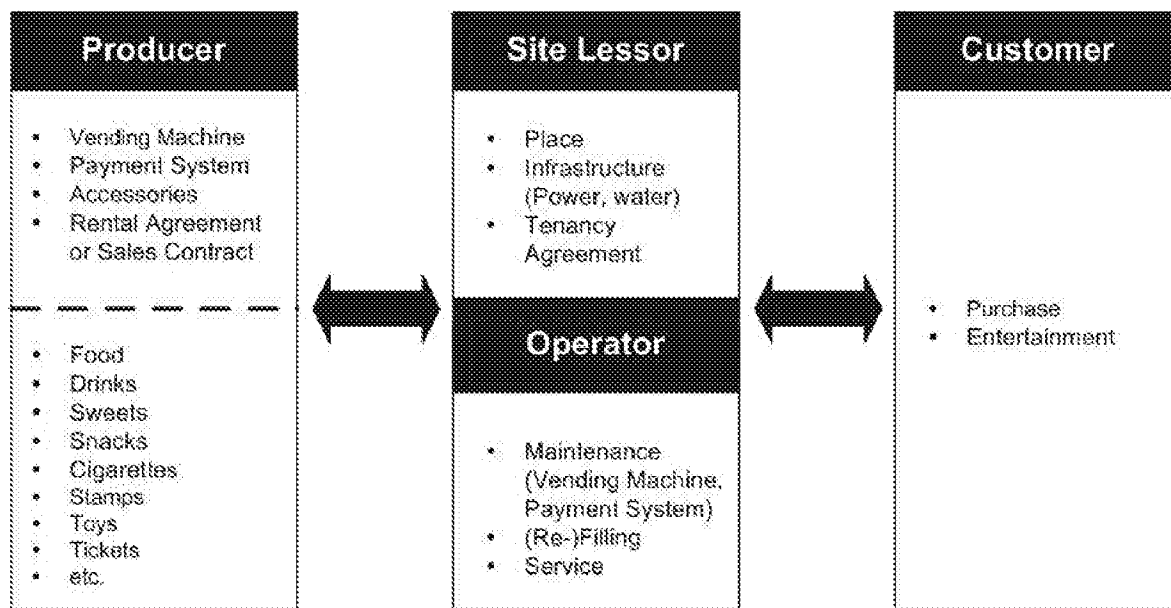
In the US, a vending machine utilizes a full glass front to merchandise the product selection inside the machine. Most often the product is delivered via spirals and is dispensed to a delivery pan located at the bottom of the machine.<sup>14</sup>

Summarising, in this article vending is defined as the selling of goods or services by a vending machine at which the customer has to administer the selection of the product or the service, to pick up the product and carry it away and to pay for the product or service on the spot – either in cash, by credit card or by means of other electronically available kinds of payment, e.g. text messaging.

## The Vending Market

In the vending market, four groups of players can be differentiated:

- the producers of the vending machines, the accessories and the goods, as well as the service provider,
- the site lessors,
- the operator (the merchandisers and maintenance people), and
- the customers (see figure 1).



**Figure 1: Vending Market Players**

## The Producer of the Vending Machine

Besides the technical functions (power, water supply, distribution and payment unit), marketing-relevant aspects (e.g. accessories like spoons, cups, serviettes) have to be considered for the design of the vending machines. Due to both the high costs of the maintenance and the strong influence of the functional efficiency on customer satisfaction, the technical equipment and the payment system as well as the distribution comfort are very important. Therefore, the handling features must be designed carefully, particularly to protect the vending machines against vandalism or technical breakdowns.



## **The Producer of the Merchandise**

Goods and accessories must serve both the technical demands of the vending machines (size, durability, handling) and the needs of the customers (attractiveness, simple opening to pick up selected goods, etc.). The packaging must guarantee that the goods do not break, and do not stick in the spiral when selected and delivered.

## **The Operator**

The operator has to look after the (re-)filling, the cleaning and the functional efficiency of the vending machine as well as the cost-, and benefit-efficiency of the housing.<sup>15</sup> Usually, the operator assembles the assortment and decides about the payment system (cash, credit card, internet, text messaging, etc.).

The operator has to know the needs, wants and attitudes of the customers. Without any data about customer profiles, who buys when, what, in which quantity, one cannot conclude from turnover to the actual customers' wishes and needs<sup>16</sup>. This lack of information is one of the main problems of the vending business. Thus, the customer is left alone when buying from the vending machine, and the operator very often does not know too much about the motives and attitudes of the customer. In general, it can be stated that from the point of view of the customer, the image of this distribution channel should be improved.

## **The Site Lessor**

The site lessor is the owner or tenant of the place where a vending machine is installed. He/she lets the place to the operator and gets paid for it. Usually, vending machines can be found in three different markets:

- the business market (office, factory, surgery, etc.),
- the catering market (restaurant, cafe, kiosk, etc.),
- the public market (public building, school, university, shopping mall, sports centre, railway station, airport, street, etc.).

## **The Customer and the Buying Situation**

The customer selects goods from the vending machine, pays for them either in cash, by credit card or by other means and takes the goods from the delivery unit, either for immediate or later consumption.

Purchasing from a vending machine can be seen as a particular buying situation. The customer cannot ask for any help, and he/she is doing the purchase by him-/herself without any advice from a shop assistant. If the vending procedure works well, the customer is served quite quickly. In the case of a problem, he/she has to find out how to deal with the situation. Usually, the operator's phone number is written on a sign that is affixed to the vending machine. That is, the customer has to make and to pay for the phone call and ideally the problem can be solved immediately. If the customer wants to complain about the goods' quality, the handling comfort of the delivery unit or anything else, first he/she has to figure out how she/he can get in touch with the contact person. The buying situation is characterised by indirect communication, the active search for information, and the customer's risk of leaving with the problem unsolved. On the other hand, the particular buying situation can also be seen positively. The customer can select, pick up the product, and pay without being disrupted or manipulated by a shop-assistant\*.

---

\* On the other hand, the reasons for customers not to buy goods from a vending machine are manifold. Some people prefer to be served. Moreover, in a study by Buber, R. et al. the customers argued that self-service is not as attractive and the service as well as the ambience of a cafe are more appealing (Buber, R./Ruso, B./Gadner, J./Gruber, S./Atzwanger, K. (2004): Measuring Consumer Behavior in Recreational and Sales Areas of Shopping Malls. Band 52 der Schriftenreihe Handel und Marketing (ed. by Schnedlitz, P.), Wien (interview 11, line 78).

## Types of Vending Machines

### Product-oriented and Service-oriented Vending Machines

The silent shop assistant is part of our life. 24 hours a day he/she offers different goods, e.g. photos for passports, business cards, parking tickets, condoms, cigarettes, sweets, food, hot and cold drinks. On other machines you can play a videogame, make copies, wash your clothes, make a phone call, gamble, etc.<sup>17</sup>

Vending machines can be categorized into product-oriented and service-oriented machines. Product-oriented vending machines are machines that offer both cold and hot food as well as non-food goods. This category includes packaging refund machines where the customer gets the bottle deposit back.

Service-oriented vending machines offer different kinds of services, entertainment (e.g. jukeboxes, slot machines) and non-entertainment (e.g. telephone or scales).

Figure 2 gives an overview of the different types of vending machines.

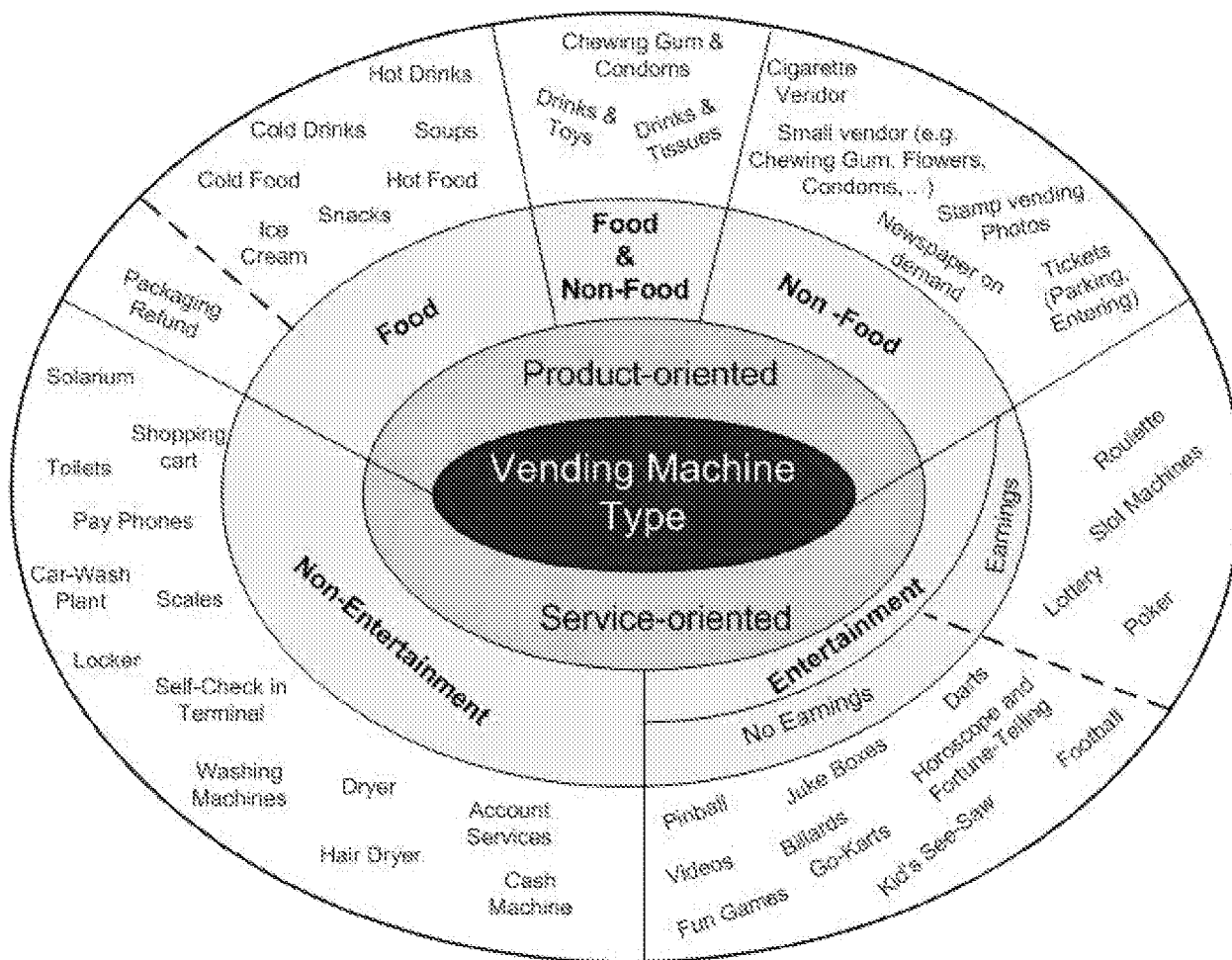
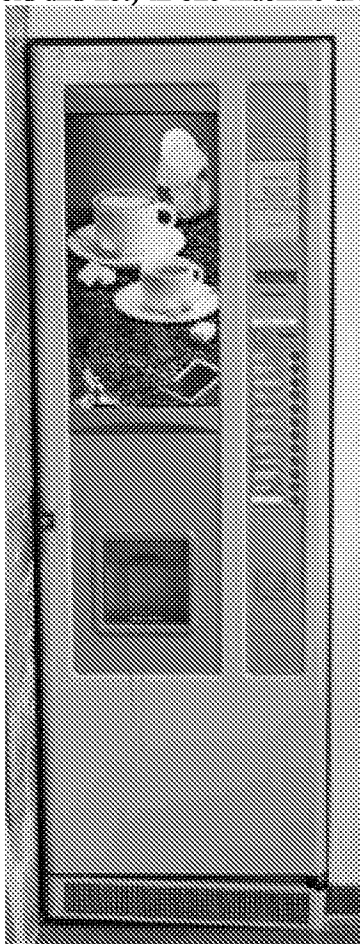


Figure 2: Types of Vending Machines and Typical Examples

## Usage of Vending Machines

### Vending Machines for Food

A food vending machine can offer either only one type of food or different kinds of food. Especially, if there is little space, combined vending machines with food (cold and hot) and drinks (cold and hot) in one machine are installed.



Vending machines for food offer:

- cold food: sandwiches, fruits, vegetables,
- hot food: fried food, pastries,
- soups,
- hot drinks: coffee, cocoa, tea, milk,
- cold drinks: ice tea, fresh juices, soft drinks, iced coffee,
- snacks: biscuits, chocolate, sweets, chewing gum, crackers, peanuts,
- ice cream.

The technical equipment for vending machines for food includes:

- Power: for all types of food,
- Water supply or water tank: for machines that offer coffee, tea, cocoa, milk, soups or fresh drinks,
- Cooling system: to cool drinks, food and ice cream,
- Heating system: to prepare hot food and keep food warm,
- Waste tanks: for the used coffee and tea powder,
- Selection panel: choice of goods
- Display: as a manual for customers
- Distribution unit: spiral rows, boxes, taps,
- Payment system: slots for coins and cards, etc.

**Figure 3: Vending Machine for Hot Drinks**

### Vending Machines for Non-Food

Figure 4 shows a typical vending machine for cigarettes and illustrates the usual applications of non-food vending machines in general.



**Figure 4: A Typical Vending Machine for Non-food Items**

Usually, vending machines for non-food offer the following items:

- cigarettes,
- flowers,
- condoms,
- toiletries (soap, towel, handkerchief, tampon, sanitary towel),
- stamps,
- photos,
- tickets: parking, entering,
- newspapers,
- toys: cars, puppets,
- small articles: jewellery, stones, stories.

The technical equipment for vending machines for non-food items includes:

- Power: for lighting and cooling equipment if necessary,
- Cooling system: to keep goods fresh,
- Selection panel: choice of goods,
- Display: as a manual for customers,
- Handing out system: spiral rows, boxes, slots,
- Payment system: slots for coins and cards.

### **Vending Machines for Food and Non-Food Items**

Figure 5 depicts a typical vending machine installed on platforms in Austrian railway stations. These machines are filled with snacks, sweets, cold drinks, and tissues.



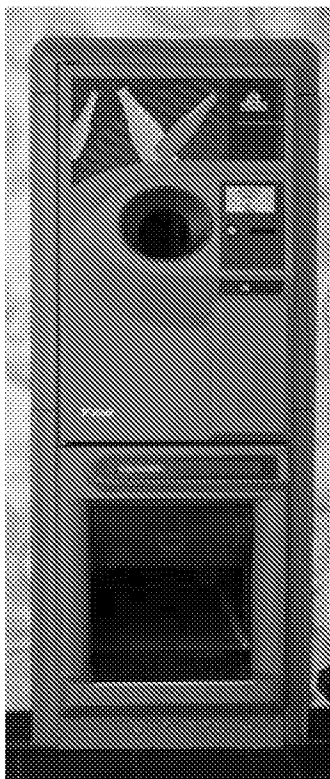
**Figure 5: Example of a Combined Vending Machine for Food and Non-Food Items**

The technical equipment for vending machines for food and non-food includes:

- Power,
- Water supply or water tank,
- Cooling system,
- Heating system,
- Waste tanks,
- Selection panel,
- Display,
- Distribution unit,
- Payment system.

### **Vending Machines for Packaging Refund**

Vending machines for packaging refund scan and register packaging like bottles, jars, cans, and boxes. The refund is paid to the customer by cash or the customer gets a ticket, which he/she has to present to the cashier.



**Figure 6: Example of a Packing Refund Machine**

The technical equipment for vending machines for packaging refund includes:

- Power: for scanning system, delivery unit,
- Scanning system: for scanning and identify the packaging,
- Handing in system: boxes, slots,
- Display,
- Printing and handing out system: printing the ticket and slots for handing out prouducts,
- Payment system: for refund.

### **Vending Machines for Non-Entertainment Services**



**Figure 7: Example of a Non-Entertainment Vending Machine**

Vending machines for non-entertainment are:

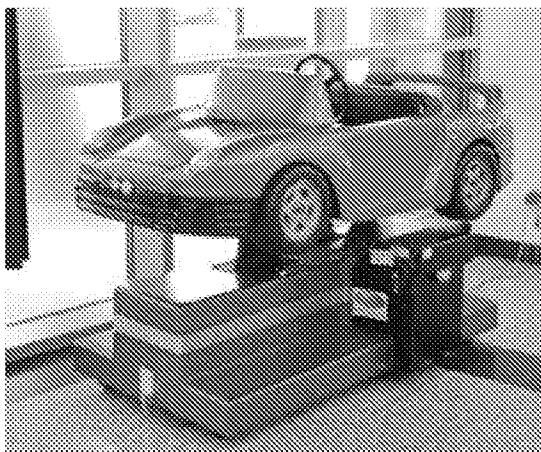
- scales,
- horoscopes and fortune-telling,
- parking and entering,
- pay phones,
- toiletries and solarium,
- shopping carts,
- banking service: foreign exchange, cash withdrawal, account services,
- lockers, safe deposits,
- check in: on airports, at railway stations,
- car service: car-wash plant, self service vacuum cleaner.

The technical equipment for vending machines for non-entertainment depends on the demands:

- Power,
- Scanning system: for check in and banking service functions,
- Display,
- Printing system: printing tickets and slots for handing out,
- Payment system:

### **Vending Machines for Entertainment – No Earnings**

If the customer has inserted the coins the vending machine starts; it ends after a fixed time or after the game is over. It can be started once again. These machines sell entertainment.



Vending machines for entertainment and no earnings are:

- sports machines: football, darts, billiards,
- fun games: pinball, video games,
- videos: on TV, in video cabins,
- jukeboxes,
- karts: go-karts for adults and children.
- automatic see-saw: animals, cars, fantasy figures.

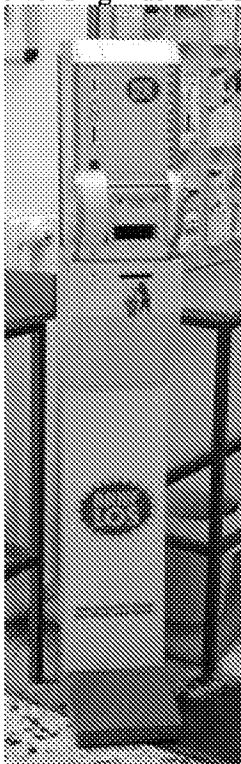
The technical equipment for vending machines for entertainment without earnings includes:

- Power: for the payment system and the engine,
- Engine: for movement,
- Display,
- Payment system.

**Figure 8: Example of an Entertainment Vending Machine (No Earnings Possible): Automatic See-Saw**

### **Vending Machines for Entertainment with Earnings**

Vending machines for entertainment with earnings are slot machines, roulette, poker, lottery, etc. These vending machines sell the game and if the customer is successful, he/she can win cash.



A vending machine for entertainment with earnings has to be equipped with the following technical items:

- Power: for the payment system and the engine,
- Engine: for movement,
- Product selection,
- Payment system: slots,
- Handing out system.

**Figure 9: Example of An Entertainment Vending Machine with Earnings**

### **Installation**

When selecting the vending machine's location one has to consider both the technical infrastructure and customer-related issues, e.g. visitor frequency, lighting, security.

Table 1 illustrates the technical demand for installing the different vending machines.

Types of Vending machines		Power 1)	Phone or Internet supply	Water supply	Cooling system	Heating system	Waste tank	Scanning system	Display	Selection panel	Distribution unit					Engine	Payment system		
											Spiral rows	Boxes	Slots	Dispenser	Accessories				
Food	Cold Food	X	(X)		X				(X)	X	c	c					X		
	Hot Food	X	(X)			X			(X)	X	c	c			c		X		
	Soups	X	(X)	X		X	X		(X)	X				X	X		X		
	Hot drinks	X	(X)	X		X	X		(X)	X				X	X		X		
	Cold drinks - juices, milk, water	X	(X)	(X)	X			X	(X)	X				X	X		X		
	Cold drinks - cans, bottles	X	(X)		X				(X)	X	X	X						X	
	Snacks	X	(X)						(X)	X	X	X						X	
	Ice cream	X	(X)	X	X			X	(X)	X				X	X			X	
	Ice - packet	X	(X)		X				(X)	X	X	X						X	
Non-Food	Cigarettes	X	(X)						(X)	X	c	c						X	
	Flowers	X	(X)		X				(X)	X		X						X	
	Condoms	X	(X)						(X)	X	c	c						X	
	Toilette articles	X	(X)						(X)	X	c	c						X	
	Stamps	X	(X)						(X)	X	c	c	c					X	
	Photos	X	(X)						(X)	X		c	c					X	
	Tickets	X	(X)						(X)	X		c	c					X	
	Newspapers	X	(X)						(X)	X	c	c	c					X	
	Toys	X	(X)						(X)	X	c	c						X	
Small articles	X	(X)						(X)	X	c	c						X		
Packaging refund	X						X	(X)			c	c					X		
Non-entertainment	Scales	(X)	(X)						X	(X)								X	
	Parking and Entering	X	(X)						(X)	(X)		c	c					X	
	Pay phones	X	X						(X)	(X)								X	
	Toilettes																	X	
	Solaries	X	(X)						(X)	X								X	
	Shopping carts																	X	
	Banking service	X	(X)					(X)	(X)	X			X					X	
	Lockers, safe deposits	(X)	(X)						(X)	(X)									X
	Check in	X	(X)					(X)	(X)	(X)			X						X
Car service	X	(X)	(X)					(X)	(X)									X	
Entertainment - No earnings	Sports machines	X	(X)						(X)	(X)							(X)	X	
	Fun games	X	(X)						(X)	(X)							(X)	X	
	Videos	X	(X)						(X)	(X)								X	
	Jukeboxes	X	(X)						(X)	(X)							(X)	X	
	Karts	X															X	X	
	Automatic See-saw	X															X	X	
	Horoscopes and fortune telling	X	(X)						(X)	(X)								X	
Entertainment - Earnings	Slot machines	X	(X)						(X)	(X)							(X)	X	
	Roulette	X	(X)						(X)	(X)							(X)	X	
	Poker	X	(X)						(X)	(X)								X	
	Lottery	X	(X)						(X)	(X)								(X)	

1 Electricity for electric operated equipment  
c one or more of the given possibilities

X is needed  
(X) depends on demands

**Table 1: The Technical Equipment of Vending Machines**

Petitioner Exhibit 1002-4173

## Future Prospects

The spectrum of vending machines is astonishingly wide: From ice-cream to hot coffee, from cigarettes to parking tickets and from train tickets to horoscopes. Further technological developments in the vending market are to be expected. Prototypes of fully automated shops, where the customers' credit cards are debited according to the goods in their trolleys at the cash point, without the help of a cashier, are already in use. These shops are, in a manner of speaking, huge vending machines and the shop assistants' tasks are reduced to merely servicing the machines. The rapid development of vending machines and the reduction of the social contact between seller and buyer mirrors two types of changes in our society. On the one hand, the technical achievements, which allow for new types of products to be offered and ensure security for both the seller and the customer. On the other hand, the customers' needs are changing. Today, on many occasions customers prefer to buy anonymously, without any personal commitment and without any time limit - twenty-four hours a day. Furthermore, as wages and rental fees are steadily increasing, shop facilities without the traditional shop assistant can be run at a more competitive price. As the customer gets more and more hybrid, he/she satisfies her/his needs by purchasing in different shop formats (from a discount store to a speciality shop) at different price levels. The customers' behavior changes dramatically, and it has to be questioned in what direction the development of purchases from vending machines will go in the future.<sup>18</sup>

## REFERENCES

- <sup>1</sup> Heron von Alexandria, in: [www.wikipedia.org](http://www.wikipedia.org), August 8, 2005, CET 13:33
- <sup>2</sup> Verkaufsautomaten, in: [www.wikipedia.org](http://www.wikipedia.org), August 8, 2005, CET 13:33
- <sup>3</sup> Tageschronik 0313, in: [www.chronikverlag.de](http://www.chronikverlag.de), August, 8, 2005, CET 13:49
- <sup>4</sup> BDV (Bundesverband Deutscher Verpflegungs- und Vending-Unternehmen e. V.) (2001): Press information, 2001, p. 1
- <sup>5</sup> Oxford University Press (1994): The Oxford English Reader's Dictionary, Berlin – Munich, p. 568
- <sup>6</sup> Photoman: Japan, in: [www.photoman.com](http://www.photoman.com), July 14, 2004, CET 14:40
- <sup>7</sup> NAMA Vision/Industry Definitions, in: [www.vending.org](http://www.vending.org), August 3, 2005, CET 12:19
- <sup>8</sup> o. V. (1999): Coffee, Candy, Cola, in: Gewerbe-Report 3/99, p. 17ff
- <sup>9</sup> NAMA Vision/Industry Definitions, in: [www.vending.org/nama\\_vision/index.php?page=definitions](http://www.vending.org/nama_vision/index.php?page=definitions), August 8, 2005, CET 16:47
- <sup>10</sup> EVA, European Vending Association: [www.eva.be](http://www.eva.be), August 3, 2005, CET 11:13
- <sup>11</sup> ÖVV, Österreichische Verkaufsautomaten Vereinigung: [www.ovv.at](http://www.ovv.at), June 16, 2005, CET 14:07
- <sup>12</sup> BDV, Bundesverband der Deutschen Vending Automaten-Wirtschaft e.V.: [www.bdv-online.de](http://www.bdv-online.de), June 16, 2005, CET 13:54
- <sup>13</sup> DILLER, H. (2001): Vahlens Großes Marketinglexikon, Verlag C. H. Beck, Munich 2001, p. 1830
- <sup>14</sup> NAMA Vision/Industry Definitions, in: [www.vending.org](http://www.vending.org), August 3, 2005, CET 12:19
- <sup>15</sup> MONSSEN, N. (1999): Vending – Ein Markt mit Zukunft. BDV (Bundesverband Deutscher Verpflegungs- und Vending-Unternehmen e. V.) (Hrsg.), Köln
- <sup>16</sup> JUNGBLUTH, H. M. (2002): High-Tech contra Anonymität. In: gv-praxis Nr. 9, 4 September 2002, p. 64 (translated by authors)
- <sup>17</sup> ÖVV: <http://www.ovv.at>, July 14, 2004, CET 16:20



<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  Substitute for Form 1449-PTO				<b>Electronically filed December 19, 2023</b>			
				Application Number		18/197,070	
				Filing Date		May 14, 2023	
				First Named Inventor		Paresh K. Patel	
				Art Unit		3698	
				Examiner Name		Frantzy POINVIL	
Sheet	1	of	16	Attorney Docket Number	104402-5074-US		

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number - Kind Code			
		4,374,557 A	2/22/1983	Sugimoto et al.	
		5,479,602 A	12/26/1995	Baecker et al.	
		5,844,808 A	12/1/1998	Konsmo et al.	
		5,854,994 A	12/29/1998	Canada et al.	
		5,880,733 A	3/9/1999	Horvitz et al.	
		5,892,900 A	4/6/1999	Ginter et al.	
		5,955,718 A	9/21/1999	Levasseur	
		6,056,194 A	5/2/2000	Kolls	
		6,390,269 B1	5/21/2002	Billington	
		6,462,644 B1	10/8/2002	Howell	
		6,505,095 B1	1/7/2003	Kolls	
		6,584,309 B1	6/24/2003	Whigham	
		6,594,759 B1	7/15/2003	Wang	
		6,743,095 B2	6/1/2004	Cole et al.	
		6,793,134 B2	9/21/2004	Clark	
		6,810,234 B1	10/26/2004	Rasanen	
		6,840,860 B1	1/11/2005	Okuniewicz	
		7,085,556 B2	8/1/2006	Offer	
		7,110,954 B2	9/19/2006	Yung et al.	
		7,127,236 B2	10/24/2006	Khan et al.	
		7,131,575 B1	11/7/2006	Kolls	
		7,455,223 B1	11/25/2008	Wilson	
		7,458,510 B1	12/2/2008	Zhou	
		7,464,867 B1	12/16/2008	Kolls	
		7,493,288 B2	2/17/2009	Bishop et al.	
		7,513,419 B1	4/7/2009	Crews et al.	
		7,672,680 B1	3/2/2010	Lee et al.	
		7,690,495 B1	4/6/2010	Kolls	
		7,721,958 B2	5/25/2010	Belfer et al.	
		7,848,980 B2	12/7/2010	Carlson	
		7,962,369 B2	6/14/2011	Rosenberg	
		7,965,693 B2	6/21/2011	Jiang et al.	
		7,983,670 B1	7/19/2011	Elliott	
		8,020,763 B1	9/20/2011	Kowalchuk	
		8,059,101 B2	11/15/2011	Westerman	
		8,157,167 B2	4/17/2012	Cost et al.	
		8,201,736 B2	6/19/2012	Majer	
		8,255,323 B1	8/28/2012	Casey et al.	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

DB2/ 47128514.1

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  Substitute for Form 1449-PTO				<b>Electronically filed December 19, 2023</b>			
				Application Number		18/197,070	
				Filing Date		May 14, 2023	
				First Named Inventor		Paresh K. Patel	
				Art Unit		3698	
				Examiner Name		Frantzy POINVIL	
Sheet	2	of	16	Attorney Docket Number	104402-5074-US		

		D669,899 S	10/30/2012	Cheng et al.	
		8,346,670 B2	1/1/2013	Hasson et al.	
		8,356,754 B2	1/22/2013	Johnson et al.	
		8,376,227 B2	2/19/2013	Hammad et al.	
		8,396,589 B2	3/12/2013	Katzenstein Garibaldi	
		8,412,626 B2	4/2/2013	Hirson et al.	
		8,438,066 B1	5/7/2013	Yuen	
		8,479,190 B2	7/2/2013	Sueyoshi et al.	
		8,489,140 B2	7/16/2013	Weiner et al.	
		8,514,775 B2	8/20/2013	Frecassetti et al.	
		8,517,766 B2	8/27/2013	Golko et al.	
		8,548,426 B2	10/1/2013	Smith	
		8,577,734 B2	11/5/2013	Treyz	
		8,583,496 B2	11/12/2013	You et al.	
		8,600,899 B1	12/2/2013	Davis	
		8,596,528 B2	12/3/2013	Fernandes et al.	
		8,596,529 B1	12/3/2013	Kolls	
		8,606,702 B2	12/10/2013	Ruckart	
		8,615,445 B2	12/24/2013	Dorsey et al.	
		8,645,971 B2	2/4/2014	Carlson et al.	
		8,700,530 B2	4/15/2014	Smith	
		8,707,276 B2	4/22/2014	Hill et al.	
		8,712,893 B1	4/29/2014	Brandmaier	
		8,761,809 B2	6/24/2014	Faith et al.	
		8,769,643 B1	7/1/2014	Ben Ayed	
		8,788,341 B1	7/22/2014	Patel	
		8,794,734 B2	8/5/2014	Drummond	
		8,810,430 B2	8/19/2014	Proud	
		8,819,659 B2	8/26/2014	Ramer et al.	
		8,831,677 B2	9/9/2014	Villa-Real	
		8,838,481 B2	9/16/2014	Moshfeghi	
		8,850,421 B2	9/30/2014	Proud	
		8,856,045 B1	10/7/2014	Patel et al.	
		8,881,975 B1	11/11/2014	Matthews	
		8,898,620 B2	11/25/2014	Eizenman et al.	
		8,903,737 B2	12/2/2014	Cameron et al.	
		8,958,846 B2	2/17/2015	Freeny, Jr.	
		9,001,047 B2	4/7/2015	Forstall	
		9,037,492 B2	5/19/2015	White	
		9,092,768 B2	7/28/2015	Breitenbach et al.	
		9,098,961 B1	8/4/2015	Block et al.	
		9,210,247 B2	12/8/2015	Vance et al.	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

DB2/ 47128514.1

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  Substitute for Form 1449-PTO				<b>Electronically filed December 19, 2023</b>			
				Application Number		18/197,070	
				Filing Date		May 14, 2023	
				First Named Inventor		Paresh K. Patel	
				Art Unit		3698	
				Examiner Name		Frantzy POINVIL	
Sheet	3	of	16	Attorney Docket Number	104402-5074-US		

		9,262,771 B1	2/16/2016	Patel	
		9,272,713 B1	3/1/2016	Dvoskin et al.	
		9,395,888 B2	7/19/2016	Schiplacoff et al.	
		9,424,603 B2	8/23/2016	Hammad	
		9,483,763 B2	11/1/2016	Van Os	
		9,547,859 B2	1/17/2017	Patel	
		9,875,473 B2	1/23/2018	Patel	
		9,898,884 B1	2/20/2018	Arora et al.	
		10,121,318 B2	11/6/2018	LeMay et al.	
		10,163,292 B1	12/25/2018	Romero	
		10,210,501 B2	2/19/2019	Low et al.	
		10,217,151 B1	2/26/2019	Greiner et al.	
		10,304,057 B1	5/28/2019	Powell	
		10,380,573 B2	8/13/2019	Lin et al.	
		10,410 194 B1	9/10/2019	Grassadonia	
		10,423,949 B2	9/24/2019	Lyons et al.	
		10,824,828 B2	11/3/2020	Ostri	
		10,977,642 B2	4/13/2021	Khan	
		11,042,852 B1	6/22/2021	Wadhwa	
		11,074577 B1	7/27/2021	Soccorsy et al.	
		11,182,794 B1	11/23/2021	Aument	
		11,227,275 B2	1/18/2022	Van Heerden et al.	
		11,373,147 B1	6/28/2022	Moore	
		11,564,266 B1	1/24/2023	Kahn	
		2002/0164953 A1	11/7/2002	Curtis	
		2003/0009385 A1	1/9/2003	Tucciarone	
		2003/0089767 A1	5/15/2003	Kiyomatsu	
		2003/0101096 A1	5/29/2003	Suzuki et al.	
		2003/0110097 A1	6/12/2003	Lei	
		2003/0130902 A1	7/10/2003	Athwal	
		2003/0158891 A1	8/21/2003	Lei et al.	
		2003/0191811 A1	10/9/2003	Hashem	
		2003/0206542 A1	11/6/2003	Holder	
		2003/0236872 A1	12/25/2003	Atkinson	
		2004/0029569 A1	2/12/2004	Khan et al.	
		2004/0049454 A1	3/11/2004	Kanno et al.	
		2004/0117262 A1	6/17/2004	Berger et al.	
		2004/0122685 A1	6/24/2004	Bunce et al.	
		2004/0133653 A1	7/8/2004	Defosse	
		2005/0021459 A1	1/27/2005	Bell	
		2005/0043011 A1	2/24/2005	Murray	
		2005/0080510 A1	4/14/2005	Bates	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

DB2/ 47128514.1

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  Substitute for Form 1449-PTO				<b>Electronically filed December 19, 2023</b>			
				Application Number		18/197,070	
				Filing Date		May 14, 2023	
				First Named Inventor		Paresh K. Patel	
				Art Unit		3698	
				Examiner Name		Frantzy POINVIL	
Sheet	4	of	16	Attorney Docket Number	104402-5074-US		

		2005/0101295 A1	5/12/2005	Rupp	
		2005/0177798 A1	8/11/2005	Thomson et al.	
		2005/0181804 A1	8/18/2005	Misikangas et al.	
		2005/0232421 A1	10/20/2005	Simons et al.	
		2005/0234776 A1	10/20/2005	Jacoves	
		2006/0043175 A1	3/2/2006	Fu et al.	
		2006/0052157 A1	3/9/2006	Walker et al.	
		2006/0123335 A1	6/8/2006	Sanchez et al.	
		2007/0050083 A1	3/1/2007	Signorelli et al.	
		2007/0083287 A1	4/12/2007	Defosse et al.	
		2007/0095901 A1	5/3/2007	Illingworth	
		2007/0119680 A1	5/31/2007	Saltsov et al.	
		2007/0159994 A1	7/12/2007	Brown et al.	
		2007/0186105 A1	8/9/2007	Bailey	
		2007/0187491 A1	8/16/2007	Godwin et al.	
		2007/0227856 A1	10/4/2007	Gopel	
		2007/0255653 A1	11/1/2007	Tumminaro	
		2008/0010193 A1	1/10/2008	Rackley III. et al.	
		2008/0010190 A1	1/10/2008	Rackley III et al.	
		2008/0033880 A1	2/7/2008	Fiebiger et al.	
		2008/0040265 A1	2/14/2008	Rackley III. et al.	
		2008/0126213 A1	5/29/2008	Robertson et al.	
		2008/0141033 A1	6/12/2008	Ginter et al.	
		2008/0154727 A1	6/26/2008	Carlson	
		2008/0154735 A1	6/26/2008	Carlson	
		2008/0163257 A1	7/3/2008	Carlson et al.	
		2008/0167017 A1	7/10/2008	Wentker et al.	
		2008/0167991 A1	7/10/2008	Carlson, et al.	
		2008/0183480 A1	7/31/2008	Carlson, et al.	
		2008/0201226 A1	8/21/2008	Carlson, et al.	
		2008/0208762 A1	8/28/2008	Arthur et al.	
		2008/0249658 A1	10/9/2008	Walker	
		2008/0254853 A1	10/16/2008	Wright et al.	
		2008/0255947 A1	10/16/2008	Friedman	
		2008/0319913 A1	12/25/2008	Wiechers	
		2009/0037284 A1	2/5/2009	Lewis et al.	
		2009/0076896 A1	3/19/2009	Dewitt	
		2009/0099961 A1	4/16/2009	Ogilvy	
		2009/0106160 A1	4/23/2009	Skowronek	
		2009/0119190 A1	5/7/2009	Realini	
		2009/0171682 A1	7/2/2009	Dixon et al.	
		2009/0287349 A1	11/19/2009	Mardiks	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  Substitute for Form 1449-PTO				<b>Electronically filed December 19, 2023</b>			
				Application Number		18/197,070	
				Filing Date		May 14, 2023	
				First Named Inventor		Paresh K. Patel	
				Art Unit		3698	
				Examiner Name		Frantzy POINVIL	
Sheet	5	of	16	Attorney Docket Number	104402-5074-US		

		2009/0288173 A1	11/19/2009	Mardiks	
		2009/0306818 A1	12/10/2009	Slagley et al.	
		2009/0306819 A1	12/10/2009	Insolia	
		2009/0303982 A1	12/10/2009	Blachman et al.	
		2009/0313132 A1	12/17/2009	Kenna et al.	
		2009/0313125 A1	12/17/2009	Roh et al.	
		2009/0327089 A1	12/31/2009	Kanno et al.	
		2010/0061294 A1	3/11/2010	Proctor Jr	
		2010/0082485 A1	4/1/2010	Lin et al.	
		2010/0094456 A1	4/15/2010	Simpkins et al.	
		2010/0105454 A1	4/29/2010	Weber et al.	
		2010/0198400 A1	8/5/2010	Pascal	
		2010/0227671 A1	9/9/2010	Laaroussi et al.	
		2010/0276484 A1	11/4/2010	Banerjee	
		2010/0280956 A1	11/4/2010	Chutorash	
		2010/0312692 A1	12/9/2010	Teicher	
		2010/0320266 A1	12/23/2010	White	
		2010/0329285 A1	12/30/2010	Stanton	
		2011/0029405 A1	2/3/2011	Cronin	
		2011/0040686 A1	2/17/2011	Carlson	
		2011/0125561 A1	5/26/2011	Marcus	
		2011/0153436 A1	6/23/2011	Krampe	
		2011/0153442 A1	6/23/2011	Krampe	
		2011/0153495 A1	6/23/2011	Dixon et al.	
		2011/0172848 A1	7/14/2011	Breitenbach et al.	
		2011/0178883 A1	7/21/2011	Granbery	
		2011/0225067 A1	9/15/2011	Dunwoody	
		2011/0238476 A1	9/29/2011	Carr	
		2011/0244799 A1	10/6/2011	Roberts et al.	
		2011/0251892 A1	10/13/2011	Laracey	
		2011/0251910 A1	10/13/2011	Dimmick	
		2011/0276636 A1	11/10/2011	Cheng et al.	
		2011/0289023 A1	11/24/2011	Forster et al.	
		2012/0011024 A1	1/12/2012	Dorsey et al.	
		2012/0016731 A1	1/19/2012	Smith et al.	
		2012/0029691 A1	2/2/2012	Mockus et al.	
		2012/0030047 A1	2/2/2012	Fuentes	
		2012/0036045 A1	2/9/2012	Lowe et al.	
		2012/0066096 A1	3/15/2012	Penide	
		2012/0078735 A1	3/29/2012	Bauer et al.	
		2012/0108173 A1	5/3/2012	Hahm et al.	
		2012/0136478 A1	5/31/2012	Anand	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  Substitute for Form 1449-PTO				<b>Electronically filed December 19, 2023</b>			
				Application Number		18/197,070	
				Filing Date		May 14, 2023	
				First Named Inventor		Paresh K. Patel	
				Art Unit		3698	
				Examiner Name		Frantzy POINVIL	
Sheet	6	of	16	Attorney Docket Number	104402-5074-US		

		2012/0150742 A1	6/14/2012	Poon et al.	
		2012/0158172 A1	6/21/2012	Wencslao	
		2012/0160912 A1	6/28/2012	Laracey	
		2012/0197740 A1	8/2/2012	Grigg et al.	
		2012/0203666 A1	8/9/2012	Torossian et al.	
		2012/0231844 A1	9/13/2012	Coppinger	
		2012/0246074 A1	9/27/2012	Annamalai et al.	
		2012/0253852 A1	10/4/2012	Pourfallah	
		2012/0254631 A1	10/4/2012	Skillman et al.	
		2012/0255653 A1	10/11/2012	Chin	
		2012/0258773 A1	10/11/2012	Alvarez Rivera	
		2012/0276845 A1	11/1/2012	Wikander	
		2012/0290472 A1	11/15/2012	Mullen et al.	
		2012/0296826 A1	11/22/2012	Bergdale et al.	
		2012/0303528 A1	11/29/2012	Weiner et al.	
		2012/0316963 A1	12/13/2012	Moshfeghi	
		2012/0330844 A1	12/27/2012	Kaufman	
		2012/0330764 A1	12/27/2012	Nahidipour	
		2013/0030931 A1	1/31/2013	Moshfeghi	
		2013/0054016 A1	2/28/2013	Canter et al.	
		2013/0054336 A1	2/28/2013	Graylin	
		2013/0054395 A1	2/28/2013	Cyr et al.	
		2013/0067365 A1	3/14/2013	Shruffi et al.	
		2013/0085835 A1	4/4/2013	Horowitz	
		2013/0087050 A1	4/11/2013	Studor et al.	
		2013/0100886 A1	4/25/2013	Cherian	
		2013/0110296 A1	5/2/2013	Khoo	
		2013/0117490 A1	5/9/2013	Harriman	
		2013/0117738 A1	5/9/2013	Livingston et al.	
		2013/0124289 A1	5/16/2013	Fisher	
		2013/0126607 A1	5/23/2013	Behjat	
		2013/0143498 A1	6/6/2013	Niemi	
		2013/0166448 A1	6/27/2013	Narayanan	
		2013/0185150 A1	7/18/2013	Crum	
		2013/0191789 A1	7/25/2013	Calman	
		2013/0217333 A1	8/22/2013	Sprigg et al.	
		2013/0246171 A1	9/19/2013	Carapelli	
		2013/0246364 A1	9/19/2013	Bhavith	
		2013/0267121 A1	10/10/2013	Hsu	
		2013/0267176 A1	10/10/2013	Hertel et al.	
		2013/0275303 A1	10/17/2013	Fiore	
		2013/0275305 A1	10/17/2013	Duplan	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

<p style="text-align: center;"><b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b></p> <p style="text-align: center;">Substitute for Form 1449-PTO</p>				<b>Electronically filed December 19, 2023</b>			
				Application Number		18/197,070	
				Filing Date		May 14, 2023	
				First Named Inventor		Paresh K. Patel	
				Art Unit		3698	
				Examiner Name		Frantzy POINVIL	
Sheet	7	of	16	Attorney Docket Number	104402-5074-US		

		2013/0278622 A1	10/24/2013	Sun et al.	
		2013/0282590 A1	10/24/2013	Rajarethnam et al.	
		2013/0297422 A1	11/7/2013	Hunter et al.	
		2013/0311379 A1	11/21/2013	Smith	
		2013/0311382 A1	11/21/2013	Fosmark et al.	
		2013/0331985 A1	12/12/2013	Felique	
		2013/0332293 A1	12/12/2013	Ran	
		2013/0346305 A1	12/26/2013	Mendes	
		2014/0006451 A1	1/2/2014	Mullis et al.	
		2014/0012414 A1	1/9/2014	Pérez et al.	
		2014/0019367 A1	1/16/2014	Khan et al.	
		2014/0025958 A1	1/23/2014	Calman	
		2014/0032413 A1	1/30/2014	Low	
		2014/0032410 A1	1/30/2014	Georgiev et al.	
		2014/0040117 A1	2/2/2014	Jain	
		2014/0040028 A1	2/6/2014	King et al.	
		2014/0052524 A1	2/20/2014	Andersen	
		2014/0052607 A1	2/20/2014	Park	
		2014/0064116 A1	3/6/2014	Linde et al.	
		2014/0067542 A1	3/6/2014	Everingham	
		2014/0074714 A1	3/13/2014	Melone et al.	
		2014/0074723 A1	3/13/2014	Kamat	
		2014/0085046 A1	3/27/2014	Shin et al.	
		2014/0085109 A1	3/27/2014	Stefik	
		2014/0089016 A1	3/27/2014	Smullin	
		2014/0100977 A1	4/10/2014	Davis	
		2014/0122298 A1	5/1/2014	Oyer	
		2014/0136301 A1	5/15/2014	Valdes	
		2014/0136411 A1	5/15/2014	Cho	
		2014/0143055 A1	5/22/2014	Johnson	
		2014/0143074 A1	5/22/2014	Kolls	
		2014/0143137 A1	5/22/2014	Carlson	
		2014/0172179 A1	6/19/2014	Baudin	
		2014/0180852 A1	6/26/2014	Kamat	
		2014/0188708 A1	7/3/2014	Govindarajan et al.	
		2014/0108108 A1	7/17/2014	Artman	
		2014/0201066 A1	7/17/2014	Roux et al.	
		2014/0249995 A1	9/4/2014	Ogilvy	
		2014/0278989 A1	9/18/2014	Calman	
		2014/0279008 A1	9/18/2014	Calman	
		2014/0279101 A1	9/18/2014	Duplan et al.	
		2014/0279556 A1	9/18/2014	Priebatsch	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

DB2/ 47128514.1

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  Substitute for Form 1449-PTO				<b>Electronically filed December 19, 2023</b>			
				Application Number		18/197,070	
				Filing Date		May 14, 2023	
				First Named Inventor		Paresh K. Patel	
				Art Unit		3698	
				Examiner Name		Frantzy POINVIL	
Sheet	8	of	16	Attorney Docket Number	104402-5074-US		

		2014/0279426 A1	9/18/2014	Holman et al.	
		2014/0289047 A1	9/25/2014	Yee	
		2014/0317611 A1	10/23/2014	Wojcik et al.	
		2014/0324627 A1	10/30/2014	Haver	
		2014/0337235 A1	11/13/2014	Van Heerden et al.	
		2014/0351099 A1	11/27/2014	Zhu	
		2014/0361872 A1	12/11/2014	Garcia et al.	
		2014/0378057 A1	12/25/2014	Ramon et al.	
		2015/0006421 A1	1/1/2015	Pearson	
		2015/0051977 A1	2/19/2015	Lyman	
		2015/0073980 A1	3/12/2015	Griffin et al.	
		2015/0081462 A1	3/19/2015	Ozvat et al.	
		2015/0088698 A1	3/26/2015	Ackerman	
		2015/0100152 A1	4/9/2015	Trevino et al.	
		2015/0105901 A1	4/16/2015	Joshi et al.	
		2015/0120546 A1	4/30/2015	Fernandes	
		2015/0120555 A1	4/30/2015	Jung	
		2015/0149992 A1	5/28/2015	Wade et al.	
		2015/0154579 A1	6/4/2015	Teicher	
		2015/0154579 A1	6/4/2015	Teicher	
		2015/0169312 A1	6/18/2015	Patel	
		2015/0170131 A1	6/18/2015	Patel	
		2015/0170132 A1	6/25/2015	Patel	
		2015/0170136 A1	6/25/2015	Patel	
		2015/0178702 A1	6/25/2015	Patel	
		2015/0220381 A1	8/6/2015	Horagan et al.	
		2015/0235202 A1	8/20/2015	Zabala	
		2015/0235202 A1	8/20/2015	Zabala	
		2015/0278811 A1	10/1/2015	Lalchandani	
		2015/0287085 A1	10/8/2015	Windmueller	
		2015/0302377 A1	10/22/2015	Sweitzer	
		2015/0317720 A1	11/5/2015	Ramaratnam	
		2015/0332029 A1	11/19/2015	Coxe	
		2015/0346994 A1	12/3/2015	Chanyontpatanakul	
		2015/0373537 A1	12/24/2015	Toksvig	
		2015/0379491 A1	12/31/2015	Ma et al.	
		2016/0012465 A1	1/14/2016	Sharp	
		2016/0019604 A1	1/21/2016	Kobayashi	
		2016/0063476 A1	3/3/2016	Baldie	
		2016/0086145 A1	3/24/2016	Tsutsui	
		2016/0092859 A1	3/31/2016	Klingen	
		2016/0098690 A1	4/7/2016	Silvia et al.	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--



INFORMATION DISCLOSURE STATEMENT BY APPLICANT				<b>Electronically filed December 19, 2023</b>	
				Application Number	18/197,070
Substitute for Form 1449-PTO				Filing Date	May 14, 2023
				First Named Inventor	Paresh K. Patel
				Art Unit	3698
				Examiner Name	Frantzy POINVIL
Sheet	9	of	16	Attorney Docket Number	104402-5074-US

		2016/0132870 A1	5/12/2016	Xu et al.	
		2016/0196220 A1	7/7/2016	Perez et al.	
		2016/0232515 A1	8/11/2016	Jhas	
		2016/0292469 A1	10/6/2016	Ianni	
		2016/0335620 A1	11/17/2016	Lyons et al.	
		2016/0350744 A1	12/1/2016	Tang et al.	
		2017/0006656 A1	1/5/2017	Nacer et al.	
		2017/0193508 A1	1/13/2017	Patel et al.	
		2017/0193478 A1	7/6/2017	Dhurka	
		2017/0193479 A1	7/6/2017	Kamat	
		2017/0330164 A1	11/16/2017	Suelberg et al.	
		2018/0005220 A1	1/4/2018	Laracey	
		2018/0165908 A1	6/14/2018	Patel et al.	
		2018/0197167 A1	7/12/2018	Ganesan et al.	
		2018/0240096 A1	8/23/2018	Patel	
		2018/0276674 A1	9/27/2018	Ramatchandirane et al.	
		2018/0315271 A1	11/1/2018	Gharabegian et al.	
		2018/0374076 A1	12/27/2018	Wheeler et al.	
		2019/0236586 A1	8/1/2019	Mei et al.	
		2019/0244205 A1	8/8/2019	Fieglein	
		2019/0244465 A1	8/8/2019	Saunders et al.	
		2020/0387881 A1	12/10/2020	Smith et al.	
		2021/0012318 A1	1/14/2021	Ducoulombier	
		2021/0056552 A1	2/25/2021	Murray	
		2021/0357932 A1	11/18/2021	Patel	
		2021/0375094 A1	12/2/2021	Thomas et al.	
		2022/0405733 A1	12/22/2022	Yao et al.	
		2023/0222506 A1	7/13/2023	Patel et al.	
		2023/0274274 A1	8/31/2023	Patel	
		2023/0289811 A1	9/14/2023	Patel et al.	
		2023/0297987 A1	9/21/2023	Patel	

**FOREIGN PATENT DOCUMENTS**

Examiner Initials	Cite No.	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Figures Appear	T
		Country Code - Number - Kind Code ( <i>if known</i> )				
		CN105139196A	12/9/2015	Shenzhen Shenruo Tech Co Ltd		
		EP1571607A2	9/7/2005	France Telecom		
		EP2061001A1	5/20/2009	Kummernuss		
		JP2002-183812A	6/28/2002	Sanyo Electric Co		
		JP2003-242401A	8/29/2003	Yoshida Sadao		

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  Substitute for Form 1449-PTO				<b>Electronically filed December 19, 2023</b>			
				Application Number		18/197,070	
				Filing Date		May 14, 2023	
				First Named Inventor		Paresh K. Patel	
				Art Unit		3698	
				Examiner Name		Frantzy POINVIL	
Sheet	10	of	16	Attorney Docket Number	104402-5074-US		

		JP2003-323662A	11/14/2003	Miyaoka Akira		
		JP2004-252640A	9/9/2004	Fuji Electric Retail Systems		
		JP2005-526325T	9/2/2005	Yeo Tae-Soon		
		JP2009-259226A	11/5/2009	Fuji Electric Retail Systems		
		JP2012-504273T	2/16/2012	Apple Inc.		
		WO2003/098561A1	11/27/2003	Yeo Tae-Soon		
		WO2007/015610A1	2/8/2007	Baek		
		WO2008/083022A1	7/10/2008	Visa USA Inc.		
		WO2008/083025A2	7/10/2008	Visa USA Inc.		
		WO2008/083078A2	7/10/2008	Visa USA Inc.		
		WO2008/083089A1	7/10/2008	Visa USA Inc.		
		WO2008/083105A2	7/10/2008	Visa USA Inc.		
		WO2008/083115A1	7/10/2008	Visa USA Inc.		
		WO2008/083119A1	7/10/2008	Visa USA Inc.		
		WO2009/070430A2	6/4/2009	Suridx, Inc.		
		WO2013/132995A1	9/12/2013	Sony		
		WO2013/177416A2	11/28/2013	Bush et al.		
		WO2014/093857A1	6/19/2014	Anderson et al.		
		WO2016/123545A1	8/4/2016	PayRange Inc.		
		WO2017/010936A1	1/19/2017	Tourego Global Pte Ltd		
		WO2017/143079A1	8/24/2017	PayRange Inc.		
		WO2006/020692A2	2/23/2006	Walker Digital, Llc		
		JP2010528716A	8/26/2010	CFPH, L. El. C.		
		KR20130138637A	12/19/2013	Lian Digital Co., Ltd.		
		WO2016158748A1	10/6/2016	NEC Corporation		
		CN106803175A	6/6/2017	Visa International Service Association		
		CN108352094A	9/7/2021	K. E. Pischick		
		JPH1125320A	1/29/1999	Fujitsu Ltd		
		JP2004310740A	11/4/2004	Kirin Beverage Corp, Kirin Brewery Co Ltd, Fuji Electric Retail Systems Co Ltd		
		JP4586607B2	11/24/2010	Oki Electric Industry Co Ltd		
		CN1561508A	1/5/2005	Swivel Secure Ltd.		
		EP3901880A1	10/27/2021	PayRange Inc.		
		WO2017010936A1	1/19/2017	Tie Wee TAN		
		CN204375056U	6/3/2015	Qingdao easy touch technology Co., Ltd.		

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

DB2/ 47128514.1

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  Substitute for Form 1449-PTO				<b>Electronically filed December 19, 2023</b>			
				Application Number		18/197,070	
				Filing Date		May 14, 2023	
				First Named Inventor		Paresh K. Patel	
				Art Unit		3698	
				Examiner Name		Frantzy POINVIL	
Sheet	11	of	16	Attorney Docket Number	104402-5074-US		

		CN107480975A	12/14/2017	Shenzhen Zhuo And Yun Klc Holdings Ltd.		
		CN207663510U	7/27/2018	Shenzhen Zhuo And Yun Klc Holdings Ltd		
		CN108367497B	6/11/2021	Microsoft Technology Licensing LLC		
		CN109389755A	2/26/2019	Fuji Electric Co., Ltd.		

**NON-PATENT LITERATURE DOCUMENTS**

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		@RobocopyEs, posted 11OCT2014, retrieved 13FEB2018, <URL:https://twitter.com/robocopyes> 2 pgs.
		Adams, How can stationary kiosks thrive in a mobile world?, American Banker, 2012
		Balan et al., mFerio: the design and evaluation of a peer-to-peer mobile payment system, JUN2009, 14 pgs
		Balfe et al., "e-EMV: emulating EMV for internet payments with trusted computing Technologies, OCT2008, 12 pgs
		Bing, Bing Images Search: "dongle", http://www.bing.com/images/search?q=dongle&FORM+HDRSC2, 05DEC2013, 8 pgs
		Carlson, Specification, US 60/871,898, 26DEC2006, 169 pgs.
		Frolick, Assessing M-Commerce Opportunities, Auerbach Publications Inc., Information Systems Management, Spring 2004
		Google, Chromecast, http://www.google.com/intl/devices/chromecast/, 12DEC2013, 4 pgs
		How to Pay the New Way, YouTube, 05APR2018, 4 pgs.
		How will Apple's new mobile wallet Passbook impact other mobile wallets?, posted 13JUN2012, retrieved 13FEB2018 from <URL:https://www.quora.com/How-will-Apples-new-mobile-wallet-Passbook-impact-other-mobile-wallets>, 5 pgs.
		Kadambi et al., Near-Field Communication-based Secure Mobile Payment Service, AUG2009, 10 pgs.
		When the Future Feels Worse Than the Past: A Temporal Inconsistency in Moral Judgment, 15 pgs. (Year: 2010) https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.675.3584&rep=rep1&type=pdf
		Novotny, Applying RFID technology in the retail industry-benefits and concerns from the consumer's perspective, Institute of Economic Science, Eszterhazy Karoly College, Eger, Hungary, Retail Technologies for the 21 Century, innovation and competitiveness in the retail industry, 2015
		Nurel, "Recent Developments in Wireless Network Systems", Izmir Institute of Technology, September 2001, 280 pages (Year: 2001).
		Patel, Office Action, US14/320,534, 02MAR2018, 26 pgs.
		Patel, Final Office Action, US14/320,534, 16APR2015, 21 pgs.
		Patel, Final Office Action, US14/320,534, 30NOV2016, 24 pgs.
		Patel, Final Office Action, US14/321,717, 18JUN2015, 22 pgs.

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				<b>Electronically filed December 19, 2023</b>	
				Application Number	18/197,070
Substitute for Form 1449-PTO				Filing Date	May 14, 2023
				First Named Inventor	Paresh K. Patel
				Art Unit	3698
				Examiner Name	Frantzy POINVIL
Sheet	12	of	16	Attorney Docket Number	104402-5074-US

		Patel, Final Office Action, US14/321,724, 08OCT2015, 19 pgs.
		Patel, Final Office Action, US14/321,724, 13DEC2017, 22 pgs.
		Patel, Final Office Action, US14/321,733, 14NOV2014, 11 pgs.
		Patel, Final Office Action, US14/335,762, 09JUN2016, 15 pgs.
		Patel, Final Office Action, US14/456,683, 08JUN2015, 14 pgs.
		Patel, Final Office Action, US14/458,192, 16SEP2015, 26 pgs.
		Patel, Final Office Action, US14/458,199, 24JUN2015, 8 pgs.
		Patel, Final Office Action, US14/641,236, 11MAR2016, 16 pgs.
		Patel, Final Office Action, US14/968,703, 12FEB2019, 22 pgs.
		Patel, Final Office Action, US15/435,228, 02OCT2020, 24 pgs.
		Patel, Final Office Action, US15/893,514, 22JUL2021, 12 pgs.
		Patel, Final Office Action, US15/956,741, 02OCT2020, 12 pgs.
		Patel, Notice of Allowance, US14/214,644, 10JUN2014, 9 pgs.
		Patel, Notice of Allowance, US14/321,733, 22JUN2015, 8 pgs.
		Patel, Notice of Allowance, US14/321,733, 27FEB2015, 9 pgs.
		Patel, Notice of Allowance, US14/335,762, 03OCT2016, 8 pgs.
		Patel, Notice of Allowance, US14/335,762, 30MAR2015, 9 pgs.
		Patel, Notice of Allowance, US14/456,683, 08OCT2015, 15 pgs.
		Patel, Notice of Allowance, US14/458,192, 12OCT2017, 8 pgs..
		Patel, Notice of Allowance, US14/458,199, 20JAN2017, 9 pgs.
		Patel, Notice of Allowance, US14/611,065, 26MAR2018, 18 pgs.
		Patel, Notice of Allowance, US14/614,336, 11DEC2015, 8 pgs.
		Patel, Notice of Allowance, US14/614,336, 25NOV2015, 13 pgs.
		Patel, Notice of Allowance, US14/968,703, 27JUN2019, 10 pgs..
		Patel, Notice of Allowance, US15/406,492, 11MAR2020, 10 pgs.
		Patel, Notice of Allowance, US15/435,228, 12AUG2021, 9 pgs.
		Patel, Notice of Allowance, US15/603,400, 18DEC2019, 9 pgs.
		Patel, Notice of Allowance, US15/603,400, 18JUN2020, 5 pgs.
		Patel, Notice of Allowance, US15/878,352, 23OCT2020, 9 pgs.
		Patel, Notice of Allowance, US16/029,483, 23DEC2020, 23 pgs.
		Patel, Notice of Allowance, US16/748,727, 09MAY2022, 18 pgs.
		Patel, Notice of Allowance, US16/748,727, 20JAN2022, 17 pgs.
		Patel, Notice of Allowance, US16/750,477, 26JAN2022, 17 pgs.
		Patel, Notice of Allowance, US16/934,933, 31MAR2021, 9 pgs.
		Patel, Notice of Allowance, US16/681,673, 17AUG2022, 22 pgs.
		Patel, Notice of Allowability, US16/934,392, 28SEP2022, 2 pgs.
		Patel, Notice of Allowance, US17/529,111, 22SEP2022, 10 pgs.
		Patel, Notice of Allowance, US17/654,732, 16SEP2022, 9 pgs.
		Patel, Non-Final Office Action, US14/320,534, 08APR2016, 21 pgs.
		Patel, Non-Final Office Action, US14/320,534, 29OCT2014, 18 pgs.
		Patel, Non-Final Office Action, US14/321,717, 19DEC2014, 16 pgs.

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

DB2/ 47128514.1

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  Substitute for Form 1449-PTO				<b>Electronically filed December 19, 2023</b>			
				Application Number		18/197,070	
				Filing Date		May 14, 2023	
				First Named Inventor		Paresh K. Patel	
				Art Unit		3698	
				Examiner Name		Frantzy POINVIL	
Sheet	13	of	16	Attorney Docket Number	104402-5074-US		

		Patel, Non-Final Office Action, US14/321,724, 13MAR2017, 21 pgs.
		Patel, Non-Final Office Action, US14/321,724, 15MAY2015, 19 pgs.
		Patel, Non-Final Office Action, US14/321,733, 21AUG2014, 9 pgs.
		Patel, Non-Final Office Action, US14/335,762, 10DEC2014, 7 pgs.
		Patel, Non-Final Office Action, US14/335,762, 18SEP2015, 13 pgs.
		Patel, Non-Final Office Action, US14/456,683, 02JAN2015, 10 pgs.
		Patel, Non-Final Office Action, US14/458,192, 23MAR2017, 26 pgs.
		Patel, Non-Final Office Action, US14/458,192, 30JAN2015, 24 pgs.
		Patel, Non-Final Office Action, US14/458,199, 05JAN2015, 7 pgs.
		Patel, Non-Final Office Action, US14/458,199, 28MAR2016, 8 pgs.
		Patel, Non-Final Office Action, US14/611,065, 03OCT2016, 19 pgs.
		Patel, Non-Final Office Action, US14/611,065, 13JUN2017, 17 pgs.
		Patel, Non-Final Office Action, US14/614,336, 27MAY2015, 17 pgs.
		Patel, Non-Final Office Action, US14/641,236, 07FEB2018, 19 pgs.
		Patel, Non-Final Office Action, US14/641,236, 29MAY2015, 10 pgs.
		Patel, Non-Final Office Action, US14/968,703, 07AUG2018, 31 pgs.
		Patel, Non-Final Office Action, US15/406,492, 25JUL2019, 17 pgs.
		Patel, Non-Final Office Action, US15/435,228, 26MAR2020, 21 pgs.
		Patel, Non-Final Office Action, US15/603,400, 12JUN2019, 11 pgs.
		Patel, Non-Final Office Action, US15/878,352, 24JAN2020, 13 pgs.
		Patel, Non-Final Office Action, US15/893,514, 29OCT2020, 17 pgs.
		Patel, Non-Final Office Action, US15/956,741, 22APR2020, 10 pgs.
		Patel, Non-Final Office Action, US15/956,741, 27DEC2021, 10 pgs.
		Patel, Non-Final Office Action, US16/029,483, 27APR2020, 28 pgs.
		Patel, Non-Final Office Action, US16/681,673, 24DEC2021, 21 pgs.
		Patel, Non-Final Office Action, US16/934,933, 28OCT2020, 10 pgs.
		Patel, Non-Final Office Action, US17/216,399, 08APR2022, 15 pgs.
		Patel, Non-Final Office Action, US15/893,514, 30SEP2022, 8 pgs.
		Pay Range Inc., Communication Pursuant to Article 94(3), EP14828617.2, 19DEC2017, 6 pgs.
		Pay Range Inc., Communication Pursuant to Article 94(3), EP16706931.9, 29JUN2018, 8 pgs.
		Pay Range Inc., Communication Pursuant to Rules 161(1) and 162, EP14828617.2, 21SEP2016, 2 pgs.
		Pay Range Inc., Communication Pursuant to Rules 161(1) and 162, EP16706931.9, 21SEP2017, 2 pgs.
		Pay Range Inc., Communication under Rule 71(3) EPC, EP14828617.2, 19NOV2020, 7 pgs.
		Pay Range Inc., Communication under Rule 71(3) EPC, EP17708929.9, 12JUN2020, 7 pgs.
		Pay Range Inc., European Search Report, EP20203134.0, 01MAR2021, 7 pgs.
		Pay Range Inc., European Search Report, EP21165692.1, 14SEP2021, 10 pgs.
		Pay Range Inc., IPRP, PCT/US2014/071284, 21JUN2016, 6 pgs.
		Pay Range Inc., IPRP, PCT/US2016/015763, 01AUG2017, 7 pgs.
		Pay Range Inc., IPRP, PCT/US2017/015676, 31JUL2018, 9 pgs.
		Pay Range Inc., IPRP, PCT/US2017/018194, 21AUG2018, 17 pgs.

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				<b>Electronically filed December 19, 2023</b>	
				Application Number	18/197,070
Substitute for Form 1449-PTO				Filing Date	May 14, 2023
				First Named Inventor	Paresh K. Patel
				Art Unit	3698
				Examiner Name	Frantzy POINVIL
Sheet	14	of	16	Attorney Docket Number	104402-5074-US

		Pay Range Inc., IPRP, PCT/US2019/060777, 11MAY2021, 7 pgs.
		Pay Range Inc., ISR/WO, PCT/US2014/071284, 25MAR2015, 9 pgs.
		Pay Range Inc., ISR/WO, PCT/US2016/015763, 08APR2016, 9 pgs.
		Pay Range Inc., ISR/WO, PCT/US2017/015676, 18APR2017, 11 pgs.
		Pay Range Inc., ISR/WO, PCT/US2017/018194, 12APR2017, 10 pgs.
		Pay Range Inc., ISR/WO, PCT/US2019/060777, 06FEB2020, 11 pgs.
		Pay Range Inc., ISR/WO, PCT/US2021/042632, 17NOV2021, 11 pgs.
		Pay Range Inc., Notice of Reasons for Rejection, JP2017527886, 29AUG2019, 10 pgs.
		Pay Range Inc., Notice of Reasons for Rejection, JP2018-543707, 04SEP2020, 4 pgs.
		Pay Range Inc., Notice of Reasons for Rejection, JP2020-101558, 07OCT2021, 4 pgs.
		Pay Range Inc., Summons to Attend Oral Proceedings, EP14828617.2, 02APR2020, 12 pgs.
		Pay Range New Product Launch, posted at youtube.com 27JUN2015, © 2016 YouTube, LLC, [online], [site visited 02MAR2016]. Available from Internet, <URL: <a href="https://www.youtube.com/watch?v=NTvvV03XFeg">https://www.youtube.com/watch?v=NTvvV03XFeg</a> , 1 pg.
		Smart Vending Machine Demo at TechCrunch Disrupt 2013, posted at youtube.com 03DEC2013, © 2016 YouTube, LLC, [online], [site visited 02MAR2016]. Available from internet, URL: <a href="https://www.youtube.com/watch?v=XEz1H-gxLj8">https://www.youtube.com/watch?v=XEz1H-gxLj8</a> >
		Square Mobile Credit Card Processing for iPhone, iPod, iPad, posted at youtube.com, posting date 30APR2011, © 2016 YouTube, LLC, [online], [site visited 02MAR2016]. Available from internet, <URL: <a href="https://www.youtube.com/watch?v=v6sKb3CFSKw">https://www.youtube.com/watch?v=v6sKb3CFSKw</a> >
		Kanapaka et al., A Stochastic Game Theoretic Model for Expanding ATM Services. <a href="https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&amp;arnumber=7395687">https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&amp;arnumber=7395687</a> , 2015, 8 pgs.
		Patel, Notice of Allowance, US17/147,305, 06OCT2022, 9 pgs.
		Hoffman et al., "New options in Wireless payments", Internet World 7.7:37 Penton Media Inc., Penton Business Media, Inc. and their subsidiaries. (Year: 2001) 5 pgs.
		Carton et al., "Framework for Mobile Payments Integration', Electronic Journal of Information Systems Evaluation, 15.1: 14-24, Academic Conferences International Limited, January. (Year: 2012), 14 pgs.
		Apriva LLC Awarded Patent for System and Method for Facilitating a Purchase Transaction using a Customer Device Beacon, June 7, 2017, Global IP News (Year: 2017), 5 pgs.
		Kumar, "Amazon gets Indian patent for auto authentication of mobile transactions", ProQuest document Id:2433007646, Financial Express, 13 August (Year:2020), 2 pgs.
		Patel, Non-Final Office Action, US17/443,802, 23DEC2022, 14 pgs.
		Patel, Non-Final Office Action, US15/956,741, 27FEB2023, 11 pgs.
		Patel et al., Notice of Allowance, US15/893,514, 10APR2023, 13 pgs.
		Heimerl et al., "Community sourcing: Engaging Local Crowds to Perform Expert Work Via Physical Kiosks", CHI '12: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, May 2012, Pages 1539-1548, 10 pgs. <a href="https://doi.org/10.1145/2207676.2208619">https://doi.org/10.1145/2207676.2208619</a>
		Patel, Notice of Allowance, US17/443,802, 28JUN2023, 8 pgs.
		Patel, Corrected Notice of Allowability, US17/443,802, 10JUL2023, 5 pgs.
		Patel, Notice of Allowance, US17/983,311, 28JUN2023, 10 pgs.
Examiner Signature		Date Considered

DB2/ 47128514.1

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  Substitute for Form 1449-PTO				<b>Electronically filed December 19, 2023</b>			
				Application Number		18/197,070	
				Filing Date		May 14, 2023	
				First Named Inventor		Paresh K. Patel	
				Art Unit		3698	
				Examiner Name		Frantzy POINVIL	
Sheet	15	of	16	Attorney Docket Number	104402-5074-US		

	EIC 3600 Search Report, STIC, Scientific & Technical Information Center, Date Completed 06/12/2023, 5 pgs.
	Patel et al., Notice of Allowance, US15/893,514, 12JUL2023, 13 pgs.
	Patel et al., Notice of Allowance, US17/973,506, 26JUL2023, 13 pgs.
	Katy Jacob, "Are mobile payments the smart cards of the aughts?", Scientific and Technical Information Center, Report Information from Dialog, July 14, 2023 – 11:33, ProQuest, Publication Info: Chicago Fed Letter 240: 1-4. Federal Reserve Bank of Chicago. (Jul 2007), 9 pgs.
	Patel et al., Notice of Allowance, US17/963,170, 04AUG2023, 16 pgs.
	USA Technologies Announces Cashless Solution to Be Offered by Blackboard Inc., Scientific and Technical Information Center, Report Information from Dialog, July 25, 2023, ProQuest, Publication Info: Business Wire 18 July 2007: NA, 6 pgs.
	Patel, Non-Final Office Action, US18/197,071, 16AUG2023, 9 pgs.
	Hossain et al., " COMPREHENSIVE STUDY OF BLUETOOTH SIGNAL PARAMETERS FOR LOCALIZATION", Department of Electrical & Computer Engineering National University of Singapore, 5 pgs. Email: {g0500774, weeseng}@nus.edu.sg.
	HANDS-FREE PROFILE 1.5, Doc. No. HFP1.5_SPEC, 2005-11-25, 93 pgs.
	DEX and MDB: A Primer For Vendors   Vending Market Watch, Feb 7th, 2008, 5 pgs. <a href="https://www.vendingmarketwatch.com/print/content/10272928">https://www.vendingmarketwatch.com/print/content/10272928</a>
	MDB Protocol V4.2 – Multi-Drop Bus – Internal Communication Protocol, MDB / ICP, Version 4.2, February 2011, 313 pgs.
	Gruber et al., "THE COMMODITY VENDING MACHINE", FORUM WARE INTERNATIONAL 2005/02, 11 pgs.
	Michael L. Kasavana, Innovative VDI Standards: Moving an Industry Forward, The Journal of International Management, Volume 4, Number 3, December 2009, 10 pgs.
	SDFL Administrative Order 2021-33, April 6, 2021, 5 pgs.
	The New York Times by David Poque, In Arrived of 2 iPhones, 3 Lessons, Sept. 17, 2013, 4 pgs. <a href="https://www.nytime.com/2013/09/18/technology/personaltech/In-Arrived-of-2-iPhones-3-Lessons.html">https://www.nytime.com/2013/09/18/technology/personaltech/In-Arrived-of-2-iPhones-3-Lessons.html</a>
	Cnet, John Thompson, How to use S Beam on your Samsung Galaxy S3, June 21, 2012, 5 pgs. <a href="https://www.cnet.com/how-to/how-to-use-s-beam-on-your-samsung-galaxy-s3/">https://www.cnet.com/how-to/how-to-use-s-beam-on-your-samsung-galaxy-s3/</a>
	iPhone, User Guide For iOS 6.1 Software, 156 pgs.
	Apple Reports Fourth Quarter Results, October 28, 2013, 4 pgs.
	Apple Announces iPhone 5s—The Most Forward - Thinking Smartphone in the World, September 10, 2013, 5 pgs.
	cNet, by Marguerite Reardon, Motion sensing comes to mobile phones, June 11, 2007, 4 pgs.
	Multi-Drop Bus – Internal Communication Protocol, MDB / ICP, Version 3, March 26, 2003, 270 pgs.
	Weidong Kou, Payment Technologies for E-Commerce, University of Hong Kong Pokfulam Road, Hong Kong, ACM Subject Classification (1998): H.4, K.4.4, J.1, 339 pgs.

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

DB2/ 47128514.1

<p style="text-align: center;">INFORMATION DISCLOSURE STATEMENT BY APPLICANT</p> <p style="text-align: center;">Substitute for Form 1449-PTO</p>				<b>Electronically filed December 19, 2023</b>	
				Application Number	18/197,070
				Filing Date	May 14, 2023
				First Named Inventor	Paresh K. Patel
				Art Unit	3698
				Examiner Name	Frantzy POINVIL
Sheet	16	of	16	Attorney Docket Number	104402-5074-US

		Specification for RFID Air Interface, EPC™ Radio-Frequency Identity Protocols, Class-1 Generation-2 UHF RFID, Protocol for Communications at 860 MHz – 960 MHz, Version 1.2.0, EPCglobal Inc., 23 October 2008, 108 pgs.
		Baier et al., "Principles of Model Checking", The MIT Press Cambridge, Massachusetts, London, England, 2008, 994 pgs.
		Patel, Notice of Allowance, US17/983,311, 04OCT2023, 11 pgs.
		Patel, Notice of Allowance, US17/443,802, 01NOV2023, 8 pgs.
		Patel et al., Notice of Allowance, US15/893,514, 08NOV2023, 13 pgs.
		Kevin Werbach et al., "Contracts Ex Machina", Articles, Faculty Scholarship, University of Michigan Law School, The University of Michigan Law School Scholarship Repository, (Year: 2017), 71 pgs. <a href="https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2936&amp;context=articles">https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2936&amp;context=articles</a>

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

DB2/ 47128514.1



Weidong Kou (Ed.)

# Payment Technologies for E-Commerce



Springer

CSC ServiceWorks – Ex. 1005  
Page 1 of 339

Petitioner Exhibit 1002-4191

## Payment Technologies for E-Commerce

**Springer-Verlag Berlin Heidelberg GmbH**

CSC ServiceWorks – Ex. 1005  
Page 3 of 339

Petitioner Exhibit 1002-4193



Weidong Kou  
Room G05, TIIB  
The University of Hong Kong  
Pokfulam Road  
Hong Kong, P. R. China  
and  
National Key Laboratory of ISN  
Xidian University  
Xi'an, 710071, P. R. China  
weidong\_kou@hotmail.com

Library of Congress Cataloging-in-Publication Data

Payment technologies for E-commerce/Weidong Kou, editor.

p. cm.

Includes bibliographical references and index

ISBN 978-3-642-07887-3 ISBN 978-3-662-05322-5 (eBook)

DOI 10.1007/978-3-662-05322-5

1. Computer security. 2. Electronic funds transfers--Security measures. 3. Electronic commerce--Security measures. I. Kou, Weidong.

QA76.9.A25P39 2003

005.8--dc21

2002044591

ACM Subject Classification (1998): H.4, K.4.4, J.1

ISBN 978-3-642-07887-3

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag Berlin Heidelberg GmbH. Violations are liable for prosecution under the German Copyright Law.

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2003

Originally published by Springer-Verlag Berlin Heidelberg New York in 2003

Softcover reprint of the hardcover 1st edition 2003

The use of general descriptive names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by the editor

Cover Design: KünkelLopka, Heidelberg

Printed on acid-free paper 45/3142SR 5 4 3 2 1 0

# Table of Contents

<b>1</b>	<b>Introduction to E-Payment: An Essential Piece of the E-Commerce Puzzle</b>	
	<i>Weidong Kou</i> .....	1
1.1	Introduction .....	1
1.2	About This Book .....	3
1.3	References .....	6
<b>2</b>	<b>Security Fundamentals</b>	
	<i>Fangguo Zhang and Yumin Wang</i> .....	7
2.1	Electronic Commerce Security.....	7
2.2	Introduction to Cryptography.....	9
2.3	Symmetric Cryptosystems.....	13
2.4	Public-Key Cryptography.....	17
2.5	Digital Signatures.....	24
2.6	Cryptographic Hash Functions.....	30
2.7	Cryptographic Random Number Generators .....	31
2.8	Authentication .....	32
2.9	Summary.....	37
2.10	References.....	38
<b>3</b>	<b>Public-Key Infrastructure</b>	
	<i>Hui Li and Yumin Wang</i> .....	39
3.1	Introduction.....	39
3.2	X.509.....	50
3.3	Credential-Based PKI Systems.....	61
3.4	Summary.....	67
3.5	References.....	67
<b>4</b>	<b>Biometrics for Security in E-Commerce</b>	
	<i>David Zhang and Li Yu</i> .....	71
4.1	An Overview of Biometrics.....	71
4.2	Potential Application Areas.....	79
4.3	Multiple Authentication Technologies.....	83

4.4	How to Select a Biometrics System.....	86
4.5	Summary.....	92
4.6	References.....	92
<b>5</b>	<b>Smart Cards and Applications</b>	
	<i>Weidong Kou, Simpson Poon, and Edwin M. Knorr</i> .....	95
5.1	Introduction.....	95
5.2	Fundamentals of Smart Card Systems.....	97
5.3	Java Card.....	106
5.4	Smart Card Standards.....	109
5.5	Smart Cards and Security.....	111
5.6	Smart Card Applications.....	114
5.7	A Case Study in Smart Cards: Hong Kong's Octopus Card.....	118
5.8	Summary.....	125
5.9	References.....	126
<b>6</b>	<b>Wireless Infrastructure</b>	
	<i>Weidong Kou</i> .....	127
6.1	Introduction.....	127
6.2	Wireless Communications Infrastructure.....	128
6.3	Wireless Computing Infrastructure.....	131
6.4	Wireless Application Protocol.....	134
6.5	Wireless Security.....	144
6.6	Summary.....	145
6.7	Appendix.....	146
6.8	References.....	147
<b>7</b>	<b>Payment Agents</b>	
	<i>Amitabha Das</i> .....	149
7.1	Introduction.....	149
7.2	Security Implications of Mobile-Agent-Based Systems.....	151
7.3	Security Techniques Protecting Mobile Agents.....	151
7.4	Secure Payment Protocols Using Mobile Agents in an Untrusted Host Environment.....	156
7.5	Summary.....	168
7.6	References.....	169

<b>8</b>	<b>Digital Cash</b> <i>Yi Mu, Vijay Varadharajan, and Khanh Quoc Nguyen</i> .....	171
8.1	Introduction.....	171
8.2	Security Requirements for Digital Cash.....	172
8.3	Brands' Digital-Cash Scheme.....	173
8.4	One-Response Digital Cash.....	175
8.5	Fair Digital Cash.....	181
8.6	Summary.....	189
8.7	Appendix.....	189
8.8	References.....	192
<b>9</b>	<b>Digital Checks</b> <i>Bo Yang</i> .....	195
9.1	Introduction.....	195
9.2	Digital Check Concept.....	195
9.3	NetBill.....	199
9.4	NetCheque System.....	207
9.5	Summary.....	209
9.6	References.....	209
<b>10</b>	<b>Secure Electronic Transactions: Overview, Capabilities, and Current Status</b> <i>Gordon Agnew</i> .....	211
10.1	Introduction.....	211
10.2	Protocol Stack and Capabilities.....	212
10.3	SET Overview.....	215
10.4	SET Performance.....	223
10.5	What Lies Ahead.....	225
10.6	Summary.....	225
10.7	References.....	226
<b>11</b>	<b>Credit Card-Based Secure Online Payment</b> <i>Johnny Wong, Lev Mirlas, Weidong Kou, and Xiaodong Lin</i> .....	227
11.1	Introduction.....	227
11.2	Online Payment by Credit Card.....	228



11.3	Trust Problems in Credit Card Payments.....	230
11.4	Trusted Third Party and a Payment Protocol Using a Trusted Third Party.....	233
11.5	Summary.....	238
11.6	Appendices.....	238
11.7	References.....	243
<b>12</b>	<b>Micropayments</b>	
	<i>Amir Herzberg</i> .....	245
12.1	Introduction.....	245
12.2	Overview of Micropayment Systems.....	246
12.3	Cost Factors for Online Payments.....	250
12.4	Disputes and Chargebacks.....	252
12.5	Customer Acquiring and Support Costs.....	262
12.6	Equipment, Processing, and Communication Costs.....	273
12.7	Summary.....	279
12.8	References.....	280
<b>13</b>	<b>Industrial E-Payment Systems and Solutions</b>	
	<i>Zheng Huang, Dong Zheng, Zichen Li, and Weidong Kou</i> .....	283
13.1	Introduction.....	283
13.2	Visa Cash.....	283
13.3	iPIN E-Payment.....	289
13.4	PayPal.....	294
13.5	Summary.....	298
13.6	References.....	299
<b>14</b>	<b>Challenges and Opportunities in E-Payment</b>	
	<i>Weidong Kou</i> .....	301
14.1	E-Commerce Challenges: E-Payment Security and Privacy.....	301
14.2	E-Payment Systems Supporting Multiple Payment Methods.....	302
14.3	Smart Cards and Digital Cash.....	304
14.4	Micropayment Issues and Solutions.....	305
14.5	Summary.....	306
14.6	References.....	306

Table of Contents	ix
<b>Glossary</b> .....	309
<b>About the Editor</b> .....	323
<b>Contributors</b> .....	325
<b>Index</b> .....	331

# **1 Introduction to E-Payment: An Essential Piece of the E-Commerce Puzzle**

Weidong Kou

University of Hong Kong  
Pokfulam Road, Hong Kong

## **1.1 Introduction**

When we look at the whole picture of e-commerce, there are many pieces in the puzzle, including the Internet communication infrastructure, various web and e-commerce application servers, client browsers, products/services, databases, security and firewalls, electronic payment (or e-payment), and many other components. To make an e-commerce web storefront work, one needs to put all these pieces of the puzzle together. The first thing that happens in cyberspace is that the customer goes through the web storefront, and looks for a product/service that is interesting to him (or her). It is clear that after the customer has searched web storefront and identified products or services, the immediate next step is making the payment for the purchase of the products/services that the customer has selected. Obviously, e-payment is essential to e-commerce transactions. Without a successful e-payment step, the e-commerce picture is not complete, and very often it will not work.

Currently, the most popular method for e-payment over the Internet is credit card based e-payment. Credit cards have been widely used for mail ordering and telephone ordering. There are regulations on credit cards established by the Federal Reserve Board, the US federal agency charged with oversight of consumer credit card regulations. According to these regulations, merchants who accept credit card information in a transaction in which the credit card is not present are responsible for unauthorized transactions using the credit card information. Although the rule was developed for the mail order and telephone order context, it applies equally to the context of e-commerce over the Internet. The Federal Reserve Board's credit card regulations also limit consumer liability for unauthorized credit card transaction charges to US \$50. This limit applies to all kinds of situations whether the card is used in a face-to-face transaction, a mail order transaction, a telephone order transaction, or an e-commerce transaction over the Internet.

These federal regulations provide a regulatory framework for credit card based payment transactions over the Internet.

Given the regulatory framework, to make credit card payment work over the Internet, a technical framework has to be developed. The technical framework consists of a number of protocols/schemes to implement online credit card payment. There are two notable credit card based e-payment schemes that have been used in most retail online merchant sites. One is the combination of credit cards with the secure sockets layer (SSL) protocol, and the other is the scheme based on the secure electronic transaction (SET). The SSL protocol provides a secure communication channel between the web browser of an online customer and the e-commerce server at an online merchant site. The SSL is based on public-key infrastructure (PKI). The SET is a standard for online credit card payment. Derived from IBM's internet payment protocol (iKP), the SET was developed jointly by Visa and MasterCard in collaboration with major IT companies such as IBM, GTE, Microsoft, SAIC (Science Applications International Corporation), Terisa Systems, and Verisign. The SET standard offers a much higher level of security than the SSL-based scheme by adding much stronger security protection against fraud and unauthorized use of credit card information. The strong security protection comes with the expense of adding more complex cryptographic operations that may require additional computation resources. The additional cryptographic operations can either make the average end user's system slow to respond to the e-payment transaction, which for the end user is not tolerable, or it simply exceeds the processing capacity of the end user's system. These problems together with business issues have contributed a slow adoption of the SET standard. The SSL-based scheme has, on the other hand, become the de facto standard for online credit card payment despite that it only provides minimal security for credit card payment transaction for this over the Internet. The main reasons are that the SSL is relatively simple, the response time of an SSL-based credit card transaction is acceptable to the average user, and the existing regulatory framework of the credit card system supplements the strong protection in the SET standard to make the SSL-based credit card online payment scheme meet the current minimum requirements of online merchants, online customers, and financial institutions [1.1-1.8].

In addition to credit card based online payment, there are other e-payment methods, including digital check, digital cash, e-payment based on debit cards, smart cards, prepaid cards, pay-by-phone service, and micropayments [1.1-1.8]. Some of these e-payment methods are briefly described as below.

- **Digital check:** Digital check is a paper-check-like payment scheme. With a digital check system in place, funds can be transferred from the payer's bank account to the payee's bank account at the time the transaction takes place. Digital check is based on a bank-account debit system. The requirements for digital check systems include the assurance of a high level of security, the capability of handling different volumes (from large to

small), digital check processing efficiency, low cost of writing a digital check, and the availability to customers through a variety of service providers.

- **Digital cash:** Digital cash is based on credit and cash-payment systems. A digital cash system usually consists of a client, a merchant, and a bank. The client obtains digital cash from the bank and pays the merchant for the goods or services that he (or she) is purchasing. The properties of digital cash include anonymity, transferability, untraceability, infinite duration, portability, and double-spending protection.
- **Smart cards:** Smart cards are plastic cards with an embedded integrated circuit. When smart cards are used as a payment vehicle, they can be used either as a prepaid card with a fixed monetary value, or as a reloadable card (that is, electronic purse) into which people can reload a monetary value from time to time.
- **Micropayment:** Micropayment deals with a very small payment, typically in the range from one cent to a few dollars. Sometimes, the payment can be even a fraction of one cent. Micropayment is perhaps a new payment method born with e-commerce over the Internet. "Pay per click" for a piece of music or video, or pay for a piece of real-time information related to a particular company or company's stock is a new phenomenon in the Internet age. Traditional credit cards or other payment methods will not work, as there is a minimum charge for processing the payment that could exceed the value of a micropayment transaction.

When we look beyond e-commerce applications in web storefronts, nowadays, transferring business services onto the Web has become a trend in various industries, particularly given the recent technological developments in the areas of Web Services and Semantic Web. The idea of virtual communities is becoming a reality, as evidenced by many such communities in cyberspace having been built in the last few years, from educational hubs to virtual shopping centers. The latest technological advances in complex online services have required stronger security and more convenience in online payment over the Internet. The challenge is how to meet this increasing demand to produce new e-payment systems/solutions.

## 1.2 About This Book

This book is meant to respond to the need for a book that can provide readers with comprehensive information on advances in e-payment technology for e-commerce.

We have invited leading experts across the globe, from North America to the Middle East, from Australia and Singapore to Hong Kong and China, to contribute to this book. Starting with fundamental security, the book covers the major subjects related to e-payment, including public key infrastructure, security based on biometrics, smart cards, wireless infrastructure, payment agents, digital cash, digital checks, a secure online payment protocol using a trusted third party, SET, and micropayment.

The target audience of this book includes e-commerce and e-business developers, business managers, academic researchers, university students, professors, and professional consultants. This book can also be used for e-payment classes and training courses.

The book has been divided into roughly two parts. The first part from Chapter 2 to Chapter 7 covers the infrastructure for secure e-payment over the Internet. The second part from Chapter 8 to Chapter 13 covers a variety of e-payment methods and e-payment systems/solutions.

Security is one of the major emphases of this book. The focus of Chapters 2-4 is on security. The security requirements for e-payment or e-commerce in general, such as message privacy, message integrity, authentication, authorization, non-repudiation, and secure payment, are covered in Chapter 2. In addition, in Chapter 2, the cryptography algorithms and cryptanalysis are also discussed. Chapter 3 is mainly for the discussion of public-key infrastructure (PKI), including certificate authorities (CAs) and the ITU X.509 authentication framework. The authors of Chapter 3 have also covered the recent development of credential-based PKI systems such as simple distributed security infrastructure (SDSI) and simple public-key infrastructure (SPKI). Biometrics, such as fingerprint, retina-scan, facial scan, and voice scan, can be used to strengthen the security. In Chapter 4, a comprehensive overview of biometric technologies is provided. The potential applications of biometrics, including e-commerce applications, are discussed.

Smart cards and applications for security and e-payment are presented in Chapter 5. Smart card topics include fundamentals of smart card systems, Java Card, smart card standards, smart card security, and various smart card applications including e-payment. The Hong Kong Octopus Card, a real-life example of successful smart cards, is presented as a case study of smart cards and related applications.

With the advance of wireless technologies, e-commerce is moving to the wireless world. Wireless payment (or mobile payment) is gaining popularity. Wireless infrastructure is covered in Chapter 6, including wireless communication infrastructure, wireless computing infrastructure, wireless application protocol, and wireless security.

Chapter 7 is devoted to payment agents. A software agent is a software program that acts autonomously on behalf of a person or organization. It is very interesting to know how these software agents can be used for personalization to help us to conduct e-commerce and to make payments online. Chapter 7 covers agent systems for e-commerce and the use of agents for payment. The security implications of mobile-agent-based systems are examined. Various security techniques for protecting mobile agents are also described, followed by a detailed discussion on how to use mobile agents in an untrusted environment to conduct secure payment.

Starting with Chapter 8, the book covers a variety of e-payment methods. The authors of Chapter 8 discuss various digital cash schemes, including Brands' digital cash scheme, one-response digital cash scheme, and fair digital cash scheme. Digital checks are covered in Chapter 9. The subjects include the fundamentals of digital checks and two digital check examples: NetBill and NetCheque. Chapter 10 covers the SET standard with a detailed SET overview. The current status is reported, and the performance issue of the SET standard is discussed. The improvement of the SET standard can be made through the use of alternative PKI systems, such as elliptic curve cryptosystem (ECC). A general introduction to credit-card-based online payment is provided in Chapter 11. In addition, an innovative secure online payment protocol using a trusted third party is also described. This protocol supports privacy protection, as the order information is not released to the third party. A patent application based on this protocol has been filed. Extensive coverage of micro-payment is provided in Chapter 12, including an overview of micro-payment systems, analysis of cost factors for online payments, disputes and charge-backs, customer acquisition and support costs, equipment, and processing and communication costs.

After the discussion of a variety of e-payment methods, in Chapter 13, three systems/solutions of e-payment are introduced, including Visa Cash, iPIN, and PayPal, with descriptions of features, advantages, disadvantages, and security mechanisms.

Finally, the book concludes with Chapter 14, in which challenges and opportunities in e-payment are identified and presented. In particular, we discussed privacy and security issues, multiple payment methods, smart cards and digital cash, and micropayment.

The readers can take advantage of the structure of the book. If they have no background knowledge of security, then they can read chapters of this book sequentially; if they are already familiar with security and PKI, they can escape reading Chapters 2-3; or if they want to focus on payment methods only, they can directly go to Chapter 8, and start their reading from there. Of course, the readers, as they wish, can always select a chapter to read without a particular order.

### 1.3 References

- [1.1] W. Kou, Y. Yesha (2002) Editorial of special issue on technological challenges in electronic commerce. *Int J Digit Libr* 3: 277–278.
- [1.2] W. Kou, Y. Yesha, C. J. Tan (eds.) (2001) *Electronic commerce technologies*. LNCS 2040. Springer, Berlin Heidelberg New York.
- [1.3] W. Kou, Y. Yesha (eds.) (2000) *Electronic commerce technology trends: challenges and opportunities*. IBM Press, Carlsbad.
- [1.4] W. Kou (1997) *Networking security and standards*. Kluwer, Boston Dordrecht London.
- [1.5] M. H. Sherif (2000) *Protocols for secure electronic commerce*. CRC Press, Boca Raton London New York Washington DC.
- [1.6] M. Shaw, R. Blanning, T. Strader, A. Whinston (2000) *Handbook on electronic commerce*. Springer, Berlin Heidelberg New York.
- [1.7] D. O'Mahony, M. Peirce, H. Tewari (1997) *Electronic payment systems*. Artech House, Boston London.
- [1.8] P. Wayner (1997) *Digital cash* (2nd ed.). AP Professional, Boston New York London.



## **2 Security Fundamentals**

Fanguo Zhang and Yumin Wang

National Key Laboratory of ISN  
Xidian University, Xi'an, China

### **2.1 Electronic Commerce Security**

Since the creation of the World Wide Web (WWW), Internet-based electronic commerce has been transformed from a mere idea into reality. The Internet and similar networks provide new infrastructures for communications and commerce. These open networks interconnect computers across many different organizations with dramatically lower communications and distributed-applications development costs. This motivates businesses to transfer commercial activity from closed private networks to open networks like the Internet. Electronic commerce is classified into several forms. Business to business (B2B), business to consumer (B2C), and business to government (B2G) represent the most significant forms in terms of value.

All traditional commercial activities use procedures or occur within contexts designed to generate trust between individuals or between businesses. These trust mechanisms reduce the commercial risks faced by traders and rely on a variety of factors from prior track records, reputations, and the legal context for an exchange. However, unlike discrete face-to-face transactions where some goods are exchanged for cash, electronic commerce creates both opportunities and difficulties for potential traders. Specifically, it opens the opportunity to expand trade at lower costs in a larger marketplace distributed over a wider geographic scope. Indeed, leveraging these new opportunities over an inexpensive global communications infrastructure will be one of the key benefits of electronic commerce.

Open networks like the Internet pose the new requirement of generating trust in an electronic environment. The kernel of electronic commerce is its security, which has been described in many references [2.6-2.8]. We survey the essential requirements for carrying out secure electronic commerce as follows.

- Server security

Internet commerce requires secure-server computers, computers that serve documents, files, or programs to users. Server computers with critical applications should not be vulnerable to many attacks, such as software viruses, Trojan horses (viruses that are hidden programs or documents to be activated at a later time), and unauthorized access to the network by hackers. The basic way to achieve this is to use firewalls and proxy machines. Proxy and firewall servers intermediate all Internet communications between a firm and its external environment. Every packet and/or file transferred to or from the Internet to a firm's internal machine goes through the proxy or firewall server, where the data is checked to assure that there are no known viruses or other problems.

- Message privacy (also known as confidentiality)

Message privacy is a key requirement for electronic commerce, it assures that communications between trading parties are not revealed to others as the message traverses an open network, thus, an unauthorized party cannot read or understand the message.

- Message integrity

Message Integrity is another key requirement for electronic commerce. It is important that the communications between trading parties are not altered by a malicious enemy as they traverse an open network.

- Authentication

In most contexts, the term authentication on its own is often used to mean *authentication of the sender*, which is the assurance the sender of the message was actually the person they claimed to be. Using the paper-letter analogy, authentication of the sender is primarily provided by the signature at the bottom of the page, but the general look of the document, such as the letterhead and/or watermark on the paper, is usually also taken into consideration. Other contexts in which the term *authentication* is commonly used include

- *User authentication*, which is the assurance that the user of a computer system is really who they claim to be.
- *Authentication of the receiver*, which allows the sender to be sure that the party they intend to get the message to is the one who receives it, or at least, is the only one who can understand it.

- Authorization

Authorization ensures that a party has the authority to make a transaction, or is authorized to access specific information or computer resources. Authorization excludes the risk that employees or others may make transac-

tions that create economic damage or access key information or computational resources of the organization.

- Audit mechanisms and non-repudiation

Like normal commercial transactions, audit mechanisms for electronic commerce enable the exchange parties to maintain and revisit a history or the sequence of events during a prior transaction. In electronic commerce, these audit trails could include time stamps or records by different computers at different stages of a transaction. In addition, there is a need for confirmations and acknowledgments by the various transacting parties that they have accurately received various messages and made specific commitments. Parties should not be able to repudiate their prior commitments.

- Payments and settlements

Electronic payment and settlements systems lower transaction costs for trading parties. Secure payment and settlement systems also ensure that the commitments to pay for goods or a service over electronic media are met. They are vital to widespread electronic commerce.

In most cases, authentication and non-repudiation are more important to commerce than confidentiality. The majority of business transactions are not sensitive enough to warrant the sender to pay much effort to prevent their contents from being disclosed to third parties. On the other hand, it is usually vital for the receiver of a message to be certain of the identity (or in some cases, the authority) of the sender of the message and that the message has not been altered in transit. In the event of disputes, it is also important that both the sender and the receiver of a message are able to prove later that the message was indeed sent, and thus, hold both parties to the agreement.

There are a number of ways to meet the above security requirements for secure electronic commerce. Other than server security, all the different mechanisms rely on techniques of cryptography. Cryptographic security mechanisms, including data encryption and digital signature schemes, are often used to provide these security services.

## 2.2 Introduction to Cryptography

Cryptography is the science of writing in secret code and is an ancient art. The history of cryptography dates back to circa 1900 BC where it was mainly used for military purposes. Classical cryptography is used to protect the contents of a message from being viewed by unauthorized parties. It is the art of transforming the contents of a message from its original form to one that cannot be decoded by un-

authorized parties. This ensures that the message remains incomprehensible to unauthorized eyes, even if it is intercepted. Cryptography is a field that is by no means new, but until recently, it has largely remained in the hands of the military. Usage of cryptography for civilian purposes has become more of a mainstream practice only with the advent of ubiquitous computing and public networks. With the widespread development of computer communications, many new forms of cryptography have been proposed. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet.

As we move into an information society, the technological means for global surveillance of millions of individual people are becoming available to major governments. Cryptography has become one of the main tools for privacy, trust, access control, electronic payments, corporate security, and countless other fields.

In the following, we will introduce the basics of modern cryptography. For more about the concepts and techniques of classical cryptography, we refer the reader to [2.11, 2.14, 2.16, 2.17].

### 2.2.1 Basic Concept

In cryptographic terminology, the message is called *plaintext* or *cleartext*. Encoding the contents of the message in a way that hides its contents from outsiders is called *encryption*. The encrypted message is called the *ciphertext*. The process of retrieving the plaintext from the ciphertext is called *decryption*. Encryption and decryption usually make use of a key, and the coding method is such that decryption can be performed only by knowing the proper key.

Cryptology can be broken into two subfields: cryptography and cryptanalysis. Cryptography is the art or science of keeping messages secret and cryptanalysis is the art of breaking ciphers, i.e., retrieving the plaintext without knowing the proper key.

### 2.2.2 Basic Cryptographic Algorithms

A method of encryption and decryption is called a cipher. Some cryptographic methods rely on the secrecy of the algorithms; such algorithms are only of historical interest and are not adequate for real-world needs. Modern algorithms use keys to control encryption and decryption; a message can be decrypted only if the key matches the encryption key.

There are two classes of key-based encryption algorithms, symmetric (or secret-key) and asymmetric (or public-key) algorithms. The difference is that symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key), whereas asymmetric algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key.

Symmetric algorithms can be divided into stream ciphers and block ciphers. Stream ciphers can encrypt a single bit of plaintext at one time, whereas block ciphers take a number of bits and encrypt them as a single unit.

Asymmetric ciphers (also called public-key algorithms or, generally, public-key cryptography) permit the encryption key to be public, allowing anyone to encrypt with the key, whereas only the proper recipient (who knows the decryption key) can decrypt the message. The encryption key is also called the public key and the decryption key is called the private key or secret key.

### 2.2.3 Cryptanalysis

Cryptanalysis is the art and science of recovering the plaintext of a message without knowing the proper keys. There are many cryptanalytic techniques. Some of the more important ones for a system implementer are described below [2.11, 2.15].

- **Ciphertext-only attack:** This is the situation where an attacker does not know anything about the contents of the message and must work from ciphertext only. In practice, it is quite often possible to make guesses about the plaintext, as many types of messages have fixed format headers. However, this does not work well against modern ciphers.
- **Known-plaintext attack:** The attacker knows or can guess the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext blocks using this information. This may be done by determining the key used to encrypt the data, or via some shortcut.
- **Chosen-plaintext attack:** The attacker is able to have any text he likes encrypted with the unknown key. The task is to determine the key used for encryption.
- **Man-in-the-middle attack:** This attack is relevant for cryptographic communication and key exchange protocols. The usual way to prevent the man-in-the-middle attack is to use a public-key cryptosystem capable of providing digital signatures.

- **Correlation:** Correlation between the secret key and the output of the cryptosystem is the main source of information to the cryptanalyst. In the easiest case, the information about the secret key is directly leaked by the cryptosystem. More complicated cases require studying the correlation (basically, any relation that would not be expected on the basis of chance alone) between the observed (or measured) information about the cryptosystem and the guessed key information.
- **Attack against or using the underlying hardware:** In the last few years, as more and more small mobile crypto devices have come into widespread use, a new category of attacks has become relevant which aim directly at the hardware implementation of the cryptosystem.
- **Faults in cryptosystems:** These can lead to cryptanalysis and even to the discovery of the secret key. The interest in cryptographic devices led to the discovery that some algorithms behaved very badly with the introduction of small faults in the internal computation.
- **Quantum computing:** The research on polynomial time factoring and discrete logarithm algorithms with quantum computers has caused growing interest in quantum computing. Quantum computing is a recent field of research that uses quantum mechanics to build computers that are, in theory, more powerful than modern serial computers. The power is derived from the inherent parallelism of quantum mechanics. So instead of doing tasks one at a time, as serial machines do, quantum computers can perform them all at once. Thus, it is hoped that with quantum computers we can solve problems infeasible with serial machines. The recent results of quantum computing research imply that if quantum computers could be implemented effectively, then most of public key cryptography would become history. However, they are much less effective against secret key cryptography. Current states of the art of quantum computing do not appear alarming, as only very small machines have been implemented. The theory of quantum computation shows much promise for better performance than serial computers, however, whether it will be realized in practice is an open question.
- **DNA cryptography:** Leonard Adleman, one of the inventors of the well-known RSA Cryptosystem (see Section 2.4), came up with the idea of using DNA as computers. DNA molecules could be viewed as a very large computer capable of parallel execution. This parallel nature could give DNA computers exponential speedup against modern serial computers. There are, unfortunately, problems with DNA computers, one being that the exponential speed-up requires also exponential growth in the volume of the material needed. Thus in practice DNA computers would have limits on their performance. Also, it is not very easy to build one.

There are many other cryptographic attacks and cryptanalysis techniques. However, these are probably the most important ones for an application designer. Anyone contemplating designing a new cryptosystem should have a much deeper understanding of these issues.

## 2.3 Symmetric Cryptosystems

In *secret key cryptography*, a single key is used for both encryption and decryption. As shown in Fig. 2.1, the sender uses the key to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called *symmetric encryption*.

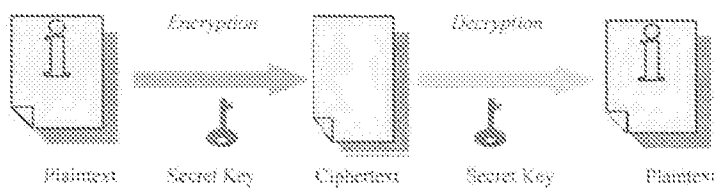


Fig. 2.1 Model of symmetric cryptosystems

With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

There are several widely used secret key cryptographic schemes, which are generally categorized as being either *block ciphers* or *stream ciphers*. A so called block cipher encrypts more than one block of data at a time; the same plaintext block will always be encrypted into the same ciphertext (when using the same key). Stream ciphers operate on a single bit, byte, or word at a time, and they implement a feedback mechanism so that the same plaintext will yield a different ciphertext every time it is encrypted.

### 2.3.1 DES and 3DES

The most common secret-key cryptography scheme used is the *data encryption standard* (DES), designed by IBM in the 1970s and adopted by the National Institute for Standards and Technology (NIST) in 1977 for commercial and unclassi-

fied government applications. DES is a block-cipher employing a 56-bit key that operates on 64-bit blocks. DES has a complex set of rules and transformations that were designed specifically to yield fast hardware implementations and slow software implementations, although this latter point is becoming less significant today since the speed of computer processors (and, therefore, programs) is several orders of magnitude faster today than twenty years ago. For many years, the US government has insisted that 56-bit DES is secure and virtually unbreakable if appropriate precautions are taken, although the cryptographic community has disagreed. On July 17, 1998, the Electronic Frontier Foundation<sup>1</sup> (EFF) announced the construction of a hardware device that could break DES in an average of 4.5 days. That device cost only about \$220,000, including design (it was erroneously and widely reported that subsequent devices could be built for as little as \$50,000). The design is scalable, which suggests that an organization could build a DES cracker that could break 56-bit keys in an average of a day for as little as \$1,000,000.

Triple DES (3DES) is a minor variation of DES. It is three times slower than regular DES but can be billions of times more secure if used properly. Triple-DES enjoys much wider use than DES because DES is so easy to break with today's rapidly advancing technology. Triple-DES defines three keys, K1, K2, and K3. Generation of the ciphertext, C, from a block of plaintext, P, is accomplished by:

$$C = E_{K3}(D_{K2}(E_{K1}(P)))$$

where  $E_K(P)$  and  $D_K(P)$  represent DES encryption and decryption, respectively, of some plaintext  $P$  using DES key  $K$ . (For obvious reasons, this is sometimes referred to as an *encrypt-decrypt-encrypt mode* operation.)

Decryption of the ciphertext is accomplished by

$$P = D_{K1}(E_{K2}(D_{K3}(C))).$$

The use of three, independent 56-bit keys provides 3DES with an effective key length of 168 bits. The specification also defines the use of two keys where, in the operations above,  $K3 = K1$ . This provides an effective key length of 112 bits. Finally, a third keying option is to use a single key, so that  $K3 = K2 = K1$ . Given the relatively low cost of key storage and the modest increase in processing due to the use of longer keys, the best recommended practices are that 3DES be employed with three keys.

Triple-DES has been adopted by ANSI as standard X9.52 and is a proposed revision to FIPS 46 as draft FIPS 46-3. NIST suggests that use of 3DES replace DES in all but legacy systems and applications.

---

<sup>1</sup> EFF website: <http://www.eff.org>



### 2.3.2 AES (Rijndael)

The AES is the Advanced Encryption Standard. The AES is the new US government standard to replace the ageing DES. The algorithm of AES is Rijndael, designed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. To quote from the NIST press release, Rijndael was selected for its “combination of security, performance, efficiency, ease of implementation, and flexibility”. With this endorsement Rijndael is quickly finding its way into readily available encryption software. Rijndael has a variable block length and key length. It uses keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192 or 256 bits (all nine combinations of key length and block length are possible). Both block length and key length can be extended very easily to multiples of 32 bits. In Daemen and Rijmen’s book [2.4], they give a detailed description of the Rijndael algorithm.

Rijndael relies more directly on algebraic constructs than do the other algorithms. Let  $GF(2^8)$  be defined by the irreducible polynomial  $x^8 + x^4 + x^3 + x + 1$ , and then view the 128 bits = 16 bytes as elements of the field. The data are placed in a  $4 \times 4$  array of elements of  $GF(2^8)$ . Rijndael has ten rounds, each consisting of four operations: ByteSub, ShiftRow, MixColumn, and AddRoundKey (the last round skips the MixColumn operation). Let elements in the array be indexed beginning with 0. ByteSub has two steps: (i) each array element is replaced by its multiplicative inverse in  $GF(2^8)$  (0 is mapped to itself), and (ii) the array undergoes a fixed affine transformation over  $GF(2^8)$ . Then ShiftRow cyclicly shifts the elements of the  $i$ th row of the array  $i$  elements to the right. In MixColumn the columns of the array are considered as polynomials over  $GF(2^8)$  (the column  $A_i = (a_{0,i}; a_{1,i}; a_{2,i}; a_{3,i})$  is viewed as the polynomial  $a_{3,i}x^3 + a_{2,i}x^2 + a_{1,i}x + a_{0,i}$ , for example) and multiplied modulo  $x^4 + 1$  by  $03x^3 + 01x^2 + 01x + 02$  to give elements of a new  $4 \times 4$  array  $B$  (thus,  $b_{0,i}$  is the zero-th degree term in the product of  $a_{3,i}x^3 + a_{2,i}x^2 + a_{1,i}x + a_{0,i}$  with  $03x^3 + 01x^2 + 01x + 02$  modulo  $x^4 + 1$ ,  $b_{1,i}$  is the coefficient of the “ $x$ ” term, etc.). MixColumn diffuses the bits of each array element through its column. RoundKey is an XOR of the key (given by the key schedule) with the elements of the array.

Rijndael admits many possibilities for parallelism: In the ByteSub and RoundKey operations the bytes can be operated on independently, and in the ShiftRow and MixColumn operations the rows and columns respectively can be independently manipulated.

The S-box (ByteSub) was designed for resistance to differential and linear cryptanalysis. It is invertible, and as it has been shown that it minimizes correlation between linear combinations of input bits and linear combinations of the output bits. MixColumn increases diffusion. Let  $x$  be a vector, and let  $A$  be a linear transformation. Define the branch number of a linear transformation as:

$$\min_{x \neq 0} \text{hwt}(x) + \text{hwt}(A(x)).$$

Since MixColumn works on columns independently, if a state has a single non-zero byte, the output can have at most four nonzero bytes. Hence the maximum branch number is 5. The polynomial  $03x^3+01x^2 + 01x + 02$  achieves this maximum.

The key schedule for Rijndael is a simple expansion using XOR and cyclic shift.

### 2.3.3 IDEA

IDEA is a 64-bit block cipher with a 128-bit key, and has an excellent reputation for quality and strength. It was originally developed in Zurich by Massey and Xuejia Lai in 1990. It was strengthened against Biham and Shamir's differential cryptanalysis attack to become IDEA in 1992.

The same algorithm is used for both encryption and decryption and consists of eight main iterations. It is based on the design concept of "mixing operations from different algebraic groups." The three algebraic groups whose operations are being mixed are: (1) XOR; (2) Addition, ignoring any overflow (addition modulo  $2^{16}$ ); and (3) Multiplication, ignoring any overflow (multiplication modulo  $2^{16}+1$ ). IDEA runs much faster in software than DES.

The main drawback of IDEA is that it is patented and requires a license for all but personal non-commercial use, specifically including internal use for normal institutional business.

### 2.3.4 Other Secret-Key Cryptography Algorithms

There are a number of other secret-key cryptography algorithms that are also in use today.

- *CAST-128* (described in Request for Comments, or RFC, 2144; CAST is not an acronym, rather, its name is derived from the initials of its inventors, Carlisle Adams and Stafford Tavares of Nortel), conceptually similar to DES, a 64-bit block cipher using 128-bit keys. A 256-bit key version has also been described, called CAST-256.
- *RC2 (RC2)*, a cipher is named for its inventor Ron Rivest (thus, "RC" is also sometimes expanded as "Ron's Code"). In addition to RC2, there are also RC4, RC5 and RC6. They all are invented by Ron Rivest. RC2 is a 64-bit block cipher using variable-sized keys designed to replace DES. Its code has not been made public although many companies have licensed RC2 for use in their products.

- *RC4*, a stream cipher uses variable-sized keys. It is widely used in commercial cryptography products, although it can only be exported using keys that are 40 bits or less in length.
- *RC5*, a block-cipher supporting a variety of block sizes, key sizes, and number of encryption passes over the data.
- *RC6*, *RC6* is based on Feistel rounds but not rounds Feistel operating between the two halves of the block. Instead, the Feistel rounds operate between pairs of quarters of the block, and they are interlocked by the exchange of some data. Circular shifts the extent of which is controlled by data, and a quadratic function applied to 32-bit integers are the nonlinear elements that provide the security of this block cipher.
- *Twofish*, a 128-bit block cipher using 128-, 192-, or 256-bit keys, invented by Bruce Schneier. Designed to be highly secure and highly flexible, well-suited for large microprocessors, 8-bit smart card microprocessors, and dedicated hardware.

## 2.4 Public-Key Cryptography

In contrast to secret-key cryptography, public-key cryptography is very new. It was first conceived of in 1976 by Diffie and Hellman [2.5], then in 1977 Rivest, Shamir and Adleman invented the RSA Cryptosystem, the first realization of a public-key system. There have since been several proposals for public-key schemes, including the ElGamal Cryptosystem and elliptic-curve cryptosystems.

Each public-key cryptosystem has its own technical nuances, however they all share the same basic property that, given an encryption key, it is computationally infeasible to determine the decryption key (and vice versa). This property lets a user, say Alice, publish her encryption key. Anyone can use that public key to encrypt a message, but only Alice can decipher the ciphertext with her private key.

In practice, computing a public-key cipher takes much longer than encoding the same message with a secret-key system. This has led to the practice of encrypting messages with a secret-key system such as DES or AES, then encoding the secret key itself with a public-key system such as RSA. We say that the public-key system “transports” the secret key. Since the secret key is usually much shorter than the message, this technique results in significantly faster processing than if public-key cryptography alone were used.

Thus, each securely transmitted message has two components: the message proper (encoded with a secret-key system) and the key used to encode the message

(itself encoded using a public-key system). Reading the message is, hence, a two-step process: first decode the secret key, then decode the message. In this chapter, when we say that a person used a public (or private) key to encrypt a message or that a message is encrypted, we are referring to this combined technique. The model of Public-key Cryptosystems (PKC) is shown in Fig 2.2.

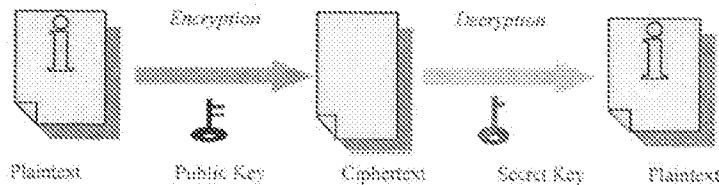


Fig. 2.2 Model of public-key cryptosystems

In a public-key cryptosystem (PKC), one of the keys is designated the *public key* and may be advertised as widely as the owner wants. The other key is designated the *private key* and is never revealed to another party. It is straight-forward to send messages under this scheme. The sender, for example, encrypts some information using the intended receiver's public key; the receiver decrypts the ciphertext using his own private key. This method could be also used in both directions at the same time. For example, the sender could encrypt the plaintext first with his own private key and then encrypt again with the receiver's public key; this latter scheme might be used where it is important that the sender cannot deny sending the message (*non-repudiation*).

Over the years, many of the proposed public-key cryptographic systems have been broken (that is, proved to be based on an easier problem than first thought), and many others have proved impractical. Today, only three types of systems should be considered both secure and efficient. The systems, classified according to the mathematical problem on which they are based, are: the *integer factorization systems* (of which RSA is the best known example), the *discrete logarithm systems* (such as the U.S. government's DSA), and the *elliptic curve cryptosystem* (also defined as the elliptic curve discrete logarithm system).

#### 2.4.1 RSA

The first, and still most common, PKC implementation is RSA, named for the three MIT mathematicians who developed it, Ronald Rivest, Adi Shamir, and Leonard Adleman [2.13]. RSA is used today in hundreds of software products and

can be used for key exchange or encryption (although the latter is relatively rare). RSA uses a variable size encryption block and a variable-size key.

When an entity, say Bob, wants to use RSA cryptosystem. He first chooses two large unique primes,  $p$  and  $q$ , of roughly equal length. Then, he computes their product  $n = pq$ , which is called the modulus. The next step is to choose a number,  $e$ , less than  $n$  and relatively prime to  $\phi(n) = (p-1)(q-1)$ , which means  $e$  and  $\phi(n)$  have no common factors except 1. In other words,  $\text{GCD}(e, \phi(n)) = 1$ . Then he finds a number  $d$  such that  $ed = 1 \pmod{\phi(n)}$ .  $e$  and  $d$  are called the public and private exponents, respectively. He publishes the public exponent and the modulus,  $(n, e)$ , and keeps  $d, p, q$  private.

Now Alice wants to send a message  $m$  to Bob. Alice computes  $c = m^e \pmod{n}$ , where  $e$  and  $n$  are Bob's public key. She sends  $c$  to Bob.

To decrypt the message  $c$  Alice has sent, Bob computes  $m$  by  $m = c^d \pmod{n}$ . The relationship between  $e$  and  $d$  ensures that Bob correctly recovers  $m$ . Because only Bob knows  $d$ , only Bob can decrypt  $c$ .

The theory behind RSA cryptosystem is that currently there are no efficient algorithms for factoring large numbers. If such algorithms are found, RSA cryptosystem will become useless.

The recommended key size for RSA cryptosystem is 1024 for normal use and 2048 for extreme security.

#### 2.4.2 Diffie-Hellman Public-Key Distribution Scheme

The Diffie - Hellman key agreement protocol was developed by Whitfield Diffie and Martin Hellman in 1976 and published in the ground-breaking paper "New Directions in Cryptography" [2.5]. The protocol allows two users to exchange a secret key over an insecure medium without any prior secrets.

The protocol has two system parameters,  $p$  and  $g$ . They are both public and may be used by all the users in a system. Parameter  $p$  is a prime number and parameter  $g$  (usually called a generator) is an integer less than  $p$ , with the following property: for every number  $h$  between 1 and  $p - 1$  inclusive, there is a power  $k$  of  $g$  such that  $h = g^k \pmod{p}$ .

Suppose Alice and Bob want to agree on a shared secret key using the Diffie-Hellman key agreement protocol. They proceed as follows: First, Alice generates a random private value  $a$  and Bob generates a random private value  $b$ . Both  $a$  and  $b$  are drawn from the set of integers  $\{1, \dots, p - 2\}$ . Then they derive their public values using parameters  $p$  and  $g$  and their private values. Alice's public value is  $g^a$

mod  $p$  and Bob's public value is  $g^b \bmod p$ . They then exchange their public values. Finally, Alice computes  $g^{ab} = (g^b)^a \bmod p$ , and Bob computes  $g^{ba} = (g^a)^b \bmod p$ . Since  $g^{ab} = g^{ba} = k$ , Alice and Bob now have a shared secret key  $k$ .

The protocol depends on the discrete logarithm problem (all of the fast algorithms known for computing discrete logarithms modulo  $p$ , where  $p$  is a large prime, are forms of the index-calculus algorithm) for its security. It assumes that it is computationally infeasible to calculate the shared secret key  $k = g^{ab} \bmod p$  given the two public values  $g^a \bmod p$  and  $g^b \bmod p$  when the prime  $p$  is sufficiently large. Maurer has shown that breaking the Diffie-Hellman protocol is equivalent to computing discrete logarithms under certain assumptions.

### 2.4.3 ECC

In 1985, Neil Koblitz [2.9] from the University of Washington and Victor Miller [2.12], who was working at IBM at that time, independently proposed the elliptic-curve cryptosystem (ECC), whose security rests on the discrete logarithm problem over the points on an elliptic curve. ECC can be used to provide both a digital signature scheme and an encryption scheme. ECC represents an alternative to older forms of public-key cryptography and offers certain advantages.

To understand what ECC entails, one must understand the arithmetic involved with elliptic curves. Elliptic curves as algebraic/geometric entities have been studied extensively for the past 150 years.

A finite field consists of a finite set of elements together with two operations, addition and multiplication, that satisfy certain arithmetic properties. Finite fields often used in cryptography are  $F_p$ ; where  $p$  is a prime number, and the field  $F_{2^m}$ .

An elliptic curve over finite field  $F_q$  consists of elements  $(x, y)$  satisfying the Weierstrass equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

When the character of  $F_q$  is not equal to 2 and 3, the equation can be simplified into

$$y^2 = x^3 + ax + b$$

If  $(x, y)$  satisfies the above equation then  $P=(x, y)$  is a point on the elliptic curve. The elliptic curve formula is slightly different for some fields.

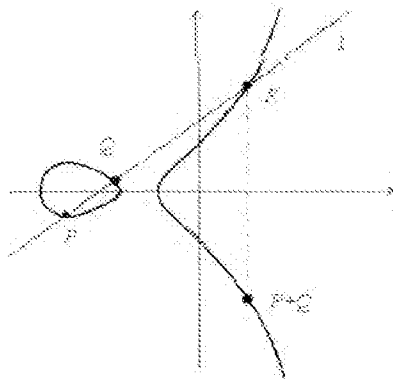


Fig. 2.3 The addition of two points on an elliptic curve

The set of points on an elliptic curve forms a group under addition, where the addition of two points on an elliptic curve is defined according to a set of simple rules. For example, consider the two points  $P$  and  $Q$  in Fig. 2.3. Point  $P$  plus point  $Q$  is equal to point  $P+Q = (x, -y)$ , where  $(x, y) = R$  is the third point on the intersection of the elliptic curve and the line  $l$  through  $P$  and  $Q$ .

The *elliptic curve discrete logarithm problem* (ECDLP) can be stated as follows. Given an elliptic curve  $E$  defined over  $\mathbb{F}_q$ , a point  $P \in E(\mathbb{F}_q)$  of order  $n$ , and a point  $Q \in E(\mathbb{F}_q)$ , determine the integer  $l$ ,  $0 \leq l \leq n - 1$ , such that  $Q = lP$ , provided that such an integer exists.

The general conclusion of leading cryptographers is that the ECDLP requires fully exponential time to solve. The security of ECC is dependent on the difficulty of solving the ECDLP.

There are several advantages to ECC [2.10]:

- ECC leads to more efficient implementations than other public-key systems due to its extra strength provided by the difficulty in solving the ECDLP.
- The biggest advantage of ECC is key size. For example, a typical key size for the RSA algorithm is 1024 bits, which would take approximately  $10^{11}$  MIPS years to break. In comparison, an ECC key size is 160 bits and offers the same level of security.
- Computational efficiencies are achieved with ECC. ECC does not require processing of prime numbers to achieve encryption, unlike other public-key cryptosystems. ECC is roughly 10 times faster than either RSA or DSA.

- ECC offers considerable bandwidth savings over the other types of public-key cryptosystems when being used to transform short messages, such as the typical implementation of ECDSA. Bandwidth savings are about the same as other public-key cryptosystems when transforming long messages.
- These advantages lead to higher speeds, lower power consumption, and code-size reductions. Implementations of ECC are particularly beneficial in applications where bandwidth, processing capacity, power availability, or storage is constrained. Such applications include wireless transactions, handheld computing, broadcast, and smart card applications.

#### 2.4.4 Other Public-Key Algorithms

##### Knapsack Cryptosystem

The Chor-Rivest knapsack cryptosystem was first published in 1984, followed by a revised version in 1988 [2.3]. It was the only knapsack-like cryptosystem that did not use modular multiplication. It was also the only knapsack-like cryptosystem that was secure for any extended period of time. Eventually, Schnorr and Hörner developed an attack on the Chor-Rivest cryptosystem using improved lattice reduction which reduced to hours the amount of time needed to crack the cryptosystem for certain parameter values (though not for those recommended by Chor and Rivest). They also showed how the attack could be extended to attack Damgård's knapsack hash function.

##### McEliece Cryptosystem

The McEliece cryptosystem is based on a class of error-correcting codes, known as Goppa codes. It was developed by R.J. McEliece in 1978. The idea behind this algorithm is to first select a particular code for which an efficient decoding algorithm is known, and then to disguise the code as a general linear code, using the fact that the problem of decoding an arbitrary linear code is NP-hard. There were no successful cryptanalytic results against the system. The system was the first public-key encryption scheme to use randomization in the encryption process. Also, the system is very efficient. But it has received little attention in practice because of some problems: the public key is enormous. The data expansion is large, and the ciphertext is twice as long as the plaintext.



## NTRU

The NTRU is a public-key cryptosystem based on the hard mathematical problem of finding very short vectors in lattices of very high dimension. It was developed by J. Hoffstein and J.H. Silverman in 1996. The process of solving this problem is called “lattice reduction”, and the general study of small vectors in lattices goes by the name “geometry of numbers”. The NTRU Cryptosystem is parameterized by three values,  $N$ ,  $p$ , and  $q$ . All objects are univariate polynomials of degree  $N$ , which are multiplied using the convolution product rule.  $p$  and  $q$  are moduli, i.e., multiplications and additions are generally followed by reduction mod  $p$  or mod  $q$ . The most time-consuming operations in the NTRU cryptosystem are the convolution multiplications. This tutorial describes ways to speed up those multiplications.

## Braid Groups Cryptosystem

The braid groups are infinite noncommutative groups naturally arisen from geometric braids. The word problem of braid groups is easy, but the generalized conjugacy search problem of braid groups is difficult. It was developed by six inventors: K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang, C.S. Park in 2000. The underlying problem of this public key cryptosystem is the generalized conjugacy search problem in the braid group and the underlying mathematical structure is the infinite noncommutative braid group  $B_n$ .

## Lucas Cryptosystem

Lucas sequences can be used for encryption and signature systems in a manner similar to RSA, but using Lucas sequences modulo a composite number instead of exponentiation. It was developed by P.J. Smith of New Zealand in 1993. It has roughly the same security as RSA for the same size key but is about twice as slow. It also has message-dependent keys. Its underlying mathematical structure is the ring of integers of the quadratic field modulo a prime  $p$ .

## Hyperelliptic Curve Cryptosystems (HCC)

Hyperelliptic curves are a special class of algebraic curves and can be viewed as generalizations of elliptic curves. A hyperelliptic curve of genus  $g = 1$  is an elliptic curve. Since 1989, the theory of hyperelliptic curves over finite fields has been applied to construction of cryptosystems. One of the main reasons for researchers interesting in cryptosystems based on elliptic and hyperelliptic curves is that these curves are a source of a tremendous number of finite abelian groups (its Jacobian) having a rich algebraic structure. Again the security depends on our inability to efficiently solve the discrete log problem, the HCDLP. The fact that this simple de-

scription of the Jacobian does not hold for curves of genus  $g > 1$  has apparently led people to shrink back from HCC. But there are compact ways to represent elements in the Jacobians and efficient algorithms to add and double in these groups.

## 2.5 Digital Signatures

Digital signatures are one of the most important applications of asymmetric public-key cryptography. They are essentially electronic signatures that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time stamped. It prevents the original signer repudiate his signature later.

A *digital signature* is a cryptographic technique that enables the user to protect digital information (represented as a bit string) from undesirable modification. Since signature cannot just be appended to a digital bit string, more sophisticated methods (also known as signatures schemes) for signing have been developed.

A signature scheme is a pair of efficient functions  $(Sig, Ver)$  of a key pair  $(S_A, V_A)$  and a bit string  $M$ , such that

- Anyone who knows the secret key  $S_A$  can efficiently compute the signature  $C = Sig(S_A, M)$  of any bit string  $M$ .
- If  $C = Sig(S_A, M)$ , then  $Ver_{V_A}(M, C) = \text{true}$ .
- For a randomly chosen  $C$ , it is intractable for anyone who does *not* know  $S_A$  to find a value  $M$  such that  $Ver_{V_A}(M, C) = \text{true}$ .

Some public-key algorithms can be used to generate digital signatures. A digital signature is a small amount of data that was created using some secret key, and there is a public key that can be used to verify that the signature was really generated using the corresponding private key. The algorithm used to generate the signature must be such that without knowing the secret key, it is not possible to create a signature that would be verified as valid.

Digital signatures are used to verify that a message really comes from the claimed sender (assuming only the sender knows the secret key corresponding to their public key). They can also be used to time stamp documents: a trusted party signs the document and its timestamp with their secret key, thus testifying that the document existed at the stated time.

### 2.5.1 Some Main Digital Signature Schemes

#### The RSA Signature Scheme

The RSA cryptosystem can perform authentication, which means it can make sure the message received is authentic, has not been tampered with, and is from the sender claimed in the message. To do that, Alice, the sender, first creates a digital signature  $s$  by  $s = m^d \bmod n$ , where  $d$  and  $n$  are Alice's private key. She then sends  $m$  and  $s$  to Bob. Upon receiving  $m$  and  $s$ , Bob can check that the message  $m$  is indeed recovered by  $m = s^e \bmod n$ , where  $e$  and  $n$  are Alice's public key.

The RSA signature scheme is a deterministic digital-signature scheme which provides message recovery. The security of the schemes presented here relies to a large degree on the intractability of the integer-factorization problem.

#### The Rabin Public-Key Signature Scheme

The Rabin signature scheme is a variant of the RSA signature scheme. It has the advantage over RSA that finding the private key and forgery are both provably as hard as factoring. Verification is faster than signing, as with RSA signatures. In the Rabin scheme, the public key is an integer  $n$  where  $n = pq$ , and  $p$  and  $q$  are prime numbers that form the private key. The message to be signed must have a square root mod  $n$ ; otherwise, it has to be modified slightly. Only about 1/4 of all possible messages have square roots mod  $n$ .

Signature:  $s = m^{1/2} \bmod n$ , where  $s$  is the signature  
 Verification:  $m = s^2 \bmod n$

The provable security has the side-effect that the prime factors can be recovered under a chosen message attack. This attack can be countered by padding a given message with random bits or by modifying the message randomly, at the loss of provable security.

#### DSA

In August of 1991, the NIST proposed a digital signature algorithm (DSA). The DSA has become a US Federal Information Processing Standard (FIPS 186), called the *digital signature standard* (DSS). It is the first digital signature scheme recognized by any government. The algorithm is a variant of the ElGamal scheme and is a digital signature scheme with appendix.

The signature mechanism requires a hash function  $h: \{0, 1\}^* \rightarrow Z_q$  for some integer  $q$ . The DSS explicitly requires use of the secure hash algorithm (SHA-1), which we will describe in Section 2.6.1.

**Key generation for the DSA [2.11].** Each entity creates a public key and corresponding private key. Each entity A should do the following:

1. Select a prime number  $q$  such that  $2^{159} < q < 2^{160}$ .
2. Choose  $t$  so that  $0 \leq t \leq 8$ , and select a prime number  $p$  where  $2^{511+64t} < p < 2^{512+64t}$ , with the property that  $q$  divides  $(p - 1)$ .
3. (Select a generator  $\alpha$  of the unique cyclic group of order  $q$  in  $Z_p^*$ .)
- 3.1 Select an element  $g \in Z_p^*$  and compute  $\alpha = g^{(p-1)/q} \bmod p$ .
- 3.2 If  $\alpha = 1$  then go to step 3.1.
4. Select a random integer  $a$  such that  $1 \leq a \leq q - 1$ .
5. Compute  $y = \alpha^a \bmod p$ .
6. A's public key is  $(p; q; \alpha; y)$ ; A's private key is  $a$ .

**DSA signature generation and verification.** In *signature generation*, entity A should do the following:

1. Select a random secret integer  $k$ ;  $0 < k < q$ .
2. Compute  $r = (\alpha^k \bmod p) \bmod q$ .
3. Compute  $k^{-1} \bmod q$ .
4. Compute  $s = k^{-1} \{h(m) + ar\} \bmod q$ .
5. A's signature for  $m$  is the pair  $(r; s)$ .

To verify A's signature  $(r; s)$  on  $m$ , B should do the following:

1. Obtain A's authentic public key  $(p; q; \alpha; y)$ .
2. Verify that  $0 < r < q$  and  $0 < s < q$ ; if not, then reject the signature.
3. Compute  $w = s^{-1} \bmod q$  and  $h(m)$ .
4. Compute  $u_1 = wh(m) \bmod q$  and  $u_2 = rw \bmod q$ .
5. Compute  $v = (\alpha^{u_1} y^{u_2} \bmod p) \bmod q$ .
6. Accept the signature if and only if  $v = r$ .

The security of the DSA relies on two distinct but related discrete logarithm problems. One is the logarithm problem in  $Z_p$ , where the powerful index-calculus methods apply; the other is the logarithm problem in the cyclic subgroup of order  $q$ , where the best current methods run in "square-root" time.

## ECDSA

A major application of ECC is ECDSA. ECC applications work extremely well with small amounts of data such as digital signatures. The ECDSA is the elliptic-curve analog of the digital signature algorithm (DSA).

The key generation procedures for ECDSA are as follows [2.9-2.10]:

1. Entity A selects an elliptic curve  $E$  defined over  $\mathbb{F}_q$ . The number of points in  $E(\mathbb{F}_q)$  should be divisible by a large prime  $n$ .
2. Select a point  $P \in E(\mathbb{F}_q)$  of order  $n$ .
3. Select a statistically unique and unpredictable integer  $d$  in the interval  $[1, n - 1]$ .
4. Compute  $Q = dP$ .
5. A's public key is  $(E, P, n, Q)$ . A's private key is  $d$ .

ECDSA signature generation:

1. Entity A selects a statistically unique and unpredictable integer  $k$  in  $[1, n - 1]$ .
2. Compute  $kP = (x_1, y_1)$  and  $r = x_1 \bmod n$ . To avoid a security condition,  $x_1$  should not equal 0.
3. Compute  $k^{-1} \bmod n$ .
4. Compute  $s = k^{-1}(h(m) + dr) \bmod n$ .  $h$  is the SHA-1.
5. If  $s = 0$ , then go to Step 1. If  $s = 0$ , then  $s^{-1} \bmod n$  does not exist and  $s^{-1}$  is required in the signature verification process.
6. The signature for the message  $m$  is the pair of integers  $(r, s)$ .

ECDSA signature verification:

1. Entity B obtains an authentic copy of entity A's public key  $(E, P, n, Q)$ .
2. Verify that  $r$  and  $s$  are integers in the interval  $[1, n - 1]$ .
3. Compute  $w = s^{-1} \bmod n$  and  $h(m)$ .
4. Compute  $u_1 = h(m)w \bmod n$  and  $u_2 = rw \bmod n$ .
5. Compute  $u_1P + u_2Q = (x_0, y_0)$  and  $v = x_0 \bmod n$ .
6. Entity B accepts the signature if and only if  $v = r$ .

Instead of choosing to generate his own elliptic curve, the entities can use the same curve  $E$  over  $\mathbb{F}_q$  and point  $P$  of order  $n$ . In this situation, an entity's public key consists of just one point  $Q$ . This results in smaller public key sizes.

### 2.5.2 Some types of digital signatures

#### Blind Digital Signature Schemes

The concept of blind signatures was introduced by Chaum [2.18] to protect the privacy of users in applications such as electronic payment systems. In contrast to regular signature schemes, a blind signature scheme is an interactive two-party protocol between a recipient and a signer. It allows the recipient to obtain a signature of a message in a way that the signer learns neither the message nor the resulting signature. A blind signature should have two requirements: *blindness* (i.e., the

signer does not know the content of the message) and *untraceability* (i.e., the signer can not link the message-signature pair after the blind signature has been revealed to the public).

### Undeniable Signature Schemes

*Undeniable signature schemes* are distinct from general digital signatures in that the signature verification protocol requires the cooperation of the signer. It is devised by Chaum and van Antwerpen [2.2], are non-self-authenticating signature schemes, where signatures can only be verified with the signer's consent. However, if a signature is only verifiable with the aid of a signer, a dishonest signer may refuse to authenticate a genuine document. Undeniable signatures solve this problem by adding a new component called the disavowal protocol in addition to the normal components of signature and verification.

### Fail-stop Signature Schemes

*Fail-stop digital signatures* are digital signatures which permit an entity A to prove that a signature purportedly (but not actually) signed by A is a forgery. This is done by showing that the underlying assumption on which the signature mechanism is based has been compromised.

The ability to prove a forgery does not rely on any cryptographic assumption, but may fail with some small probability; this failure probability is independent of the computing power of the forger. Fail-stop signature schemes have the advantage that even if a very powerful adversary can forge a single signature, the forgery can be detected and the signing mechanism no longer used. Hence, the term *fail-then-stop* is also appropriate. A fail-stop signature scheme should have the following properties:

1. If a signer signs a message according to the mechanism, then a verifier upon checking the signature should accept it.
2. A forger cannot construct signatures that pass the verification algorithm without doing an exponential amount of work.
3. If a forger succeeds in constructing a signature that passes the verification test, then with high probability, the true signer can produce a proof of forgery.
4. A signer cannot construct signatures that are at some later time claimed to be forgeries.

#### 2.5.2.4 Group Signature Schemes

In 1991 Chaum and van Heyst [2.1] put forth the concept of a group-signature scheme. Participants are group members, a membership manager, and a revocation manager. A group signature scheme allows a group member to sign messages anonymously on behalf of the group. More precisely, signatures can be verified with respect to a single public key of the group and do not reveal the identity of the signer.

The membership manager is responsible for the system setup and for adding group members, while the revocation manager has the ability to revoke the anonymity of signatures. A group signature scheme could, for instance, be used by an employee of a large company to sign documents on behalf of the company. In this scenario, it is sufficient for a verifier to know that some representative of the company has signed. Moreover, in contrast to the case when an ordinary signature scheme would be used, the verifier does not need to check whether a particular employee is allowed to sign contracts on behalf of the company, i.e., the verifier needs only to know a single company's public key.

The following informally stated security requirements must hold:

1. *Unforgeability of signatures*: Only group members are able to sign messages. Furthermore, they must only be able to sign in such a way that, when the signature is (later) presented to the revocation manager, he will be able to reveal the identity of the signer.
2. *Anonymity of signatures*: It is not feasible to find out the group member who signed a message without knowing the revocation manager's secret key.
3. *Unlinkability of signatures*: It is infeasible to decide whether two signatures have been issued by the same group member or not.
4. *No framing*: Even if the membership manager, the revocation manager, and some of the group members collude, they cannot sign on behalf of noninvolved group members.
5. *Unforgeability of tracing verification*: The revocation manager cannot falsely accuse a signer of having originated a given signature.

#### Proxy Signature Schemes

A digital signature protocol allows the signer to give the authority to sign a message to someone else without disclosing their private key.

Proxy signatures allow the signer to designate someone else to verify their signatures. In the absence of a participant, a proxy of the participant can be authorized to sign (analogous to the power of attorney concept) without even disclosing the participant's private key. This is a very strong concept for achieving privacy in a collaborative environment.

The following properties hold for proxy signatures:

- Distinguishability: Proxy signatures are distinguishable from normal signatures by everyone.
- Unforgeability: Only the signer and the authorized proxy should be able to sign.
- Verifiability: The verifier should be convinced of the proxy relationship between the participant and proxy.
- Identifiability: The original signer should be able to determine the proxy signer's identity from a proxy signature.
- Undeniability: A proxy/participant cannot deny a message.

## 2.6 Cryptographic Hash Functions

Cryptographic hash functions are used in various contexts, for example, to compute the message digest when making a digital signature. A hash function compresses the bits of a message to a fixed-size *hash value* in a way that distributes the possible messages evenly among the possible hash values. A cryptographic hash function does this in a way that makes it extremely difficult to come up with a message that would hash to a particular hash value.

Cryptographic hash functions typically produce hash values of 128 or more bits. This number ( $2^{128}$ ) is vastly larger than the number of different messages likely to ever be exchanged in the world. The reason for requiring more than 128 bits is based on the *birthday paradox*. The birthday paradox roughly states that given a hash function mapping any message to a 128-bit hash digest, we can expect that the same digest will be computed twice when  $2^{64}$  randomly selected messages have been hashed. As cheaper memory chips for computers become available, it may become necessary to require larger than 128-bit message digests (such as 160 bits, which has become standard recently).

Hash algorithms are typically used to provide a *digital fingerprint* of a file's contents, and are often used to ensure that the file has not been altered by an intruder or a virus. Hash functions are also commonly employed by many operating systems to encrypt passwords.



### 2.6.1 SHA-1

The secure hash algorithm also called the *secure hash standard* (SHS) is a cryptographic hash algorithm published by the United States Government. It produces a 160-bit hash value from a message of an arbitrary length. It is considered to be very good. The length of the padded message is a multiple of 512 bits. This standard specifies a *secure hash algorithm*, SHA-1, for computing a condensed representation of a message or a data file. When a message of any length  $< 2^{64}$  bits is input, the SHA-1 produces a 160-bit output called a message digest. The message digest can then be input to the *digital signature algorithm* (DSA), which generates or verifies the signature for the message. Signing the message digest rather than the message itself often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature.

SHA-1 is probably the preferred hash function for new applications. Currently, no problems are found from it.

### 2.6.2 MD5

The *message digest algorithm 5* (MD5) is one of message-digest algorithms developed by Rivest. The other algorithms are MD2 and MD4. MD5 is basically MD4 with “safety-belts”. While it is slightly slower than MD4, it is more secure. The algorithm consists of four distinct rounds, with a slightly different design from that of MD4. It can be used to hash an arbitrary length byte string into a 128-bit value.

MD5’s ancestor, MD4, has been broken, and there are some concerns about the safety of MD5 as well. In 1996 a collision of the MD5 compression function was found by Hans Dobbertin. Although this result does not directly compromise its security, as a precaution the use of MD5 is not recommended in new applications.

## 2.7 Cryptographic Random Number Generators

Cryptographic random number generators generate random numbers for cryptographic applications, such as keys. Conventional random number generators available in most programming languages or programming environments are not suitable for use in cryptographic applications (they are designed for statistical randomness, not to resist prediction by cryptanalysts).

In the optimal case, random numbers are based on true physical sources of randomness that cannot be predicted. Such sources may include the noise from a semiconductor device, the least significant bits of an audio input, or the intervals between device interrupts or user keystrokes. The noise obtained from a physical source is then “distilled” by a cryptographic hash function to make every bit depend on every other bit. Quite often, a large pool (several thousand bits) is used to contain randomness, and every bit of the pool is made to depend on every bit of the input noise and every other bit of the pool in a cryptographically strong way.

When true physical randomness is not available, pseudo-random numbers must be used. This situation is undesirable, but often arises on general-purposed computers. It is always desirable to obtain some environmental noise, even from device latencies, resource utilization statistics, network statistics, keyboard interrupts, or whatever. The point is that the data must be unpredictable for any external observer; to achieve this, the random pool must contain at least 128 bits of true entropy.

Cryptographic pseudo-random number generators typically have a large pool (“seed value”) containing randomness. Bits are returned from this pool by taking data from the pool, optionally running the data through a cryptographic hash function to avoid revealing the contents of the pool. When more bits are needed, the pool is stirred by encrypting its contents by a suitable cipher with a random key (that may be taken from an unreturned part of the pool) in a mode that makes every bit of the pool depend on every other bit of the pool. New environmental noise should be mixed into the pool before stirring to make prediction of previous or future values even more impossible.

Even though cryptographically strong random number generators are not very difficult to build if designed properly, they are often overlooked. The importance of the random number generator must thus be emphasized, that is, if done badly, it will easily become the weakest point of the system.

## 2.8 Authentication

In the real world of full competition, those fraudulent of identities are inevitable. One is often asked to prove one’s identity. The security of communication and data systems depend to a great extent on whether or not the identities of users can be properly verified. For instance, the *automatic teller machine* (ATM) in a bank can give cash to authorized cardholders, which improves the efficiency of the bank greatly. Access to and use of a computer and confidential data are based on the accurate verification of users’ identities. Authentication refers to a process of confirming whether or not the object to be authenticated is exactly what it is claimed to be. The object to be authenticated can be a password, a digital signa-

ture, or some physiological characteristic such as a fingerprint, voice, or retina. Authentication is often used in communication to mutually confirm the identities of users so as to guarantee to both sides that the identity of the other side is real and valid. There are many methods to realize authentication.

### 2.8.1 Authentication Based on Password

Conventional password authentication schemes involve time-invariant passwords, which provide so-called *weak authentication*. The basic idea is as follows. Each user (entity) is associated with a *password*. The user is capable of committing their password to memory. The password is then used as a shared secret between the user and the system. For the user to gain access to a system resource, he inputs a (*user-ID*, *password*) pair, and explicitly or implicitly specifies a resource. Here *user-ID* is a claim of identity, and *password* is the evidence supporting the claim. The system then authenticates the user by checking the password. The user is authentic and is authorized to access the resource if the password matches the corresponding data held for that *user-ID*.

Password schemes can be divided into many classes according to the means by which information allowing password verification is stored within the system along with the method of verification. Fixed password schemes and one-time password schemes are typical examples.

Authentication schemes based on passwords have some advantages. Many systems, such as UNIX, Windows NT, and NetWare, all support this kind of authentication. They are simple and practical for closed small systems; however, they also have disadvantages [2.11].

Password schemes are only suitable for one-way authentication. That is, the system can authenticate the user, but the user cannot authenticate the system. Hence, the adversary may disguise itself as the system to get a user's password.

To overcome these drawbacks, the system can take measures, such as enciphering the user's password when transmitting, and applying uninvertible encryption to users' password files. However, there are still some ways for the adversary to decipher a user's password or decrypt users' password files.

### 2.8.2 Double Factor Authentication

In double-factor authentication systems, a user possesses not only a password but also a device-of-access token. When a user enters the system, in addition to a password they need to also input the number showed on their device-of-access to-

ken. This number on their device-of-access token changes from time to time and is inherent with the authentication sever.

A double-factor authentication scheme is more difficult for the adversary to attack than a password-based authentication scheme. The adversary cannot pass authentication with only a user's password or access token-device. Changing numbers on the access-token device makes it even harder for the adversary to attack the system. So double-factor authentication is more secure than password-based authentication.

### 2.8.3 Two-Stage Authentication and Password-Derived Keys

Human users have difficulty remembering secret keys that have sufficient entropy to provide adequate security. Two techniques that address this issue are now described. When tokens are used with offline PIN verification, a common technique is for the PIN to serve to verify the user to the token, while the token contains additional independent information allowing the token to authenticate itself to the system (as a valid token representing a legitimate user). The user is thereby indirectly authenticated to the system by a two-stage process. This requires the users to have possession of the token but only remember a short PIN, while a longer key (containing adequate entropy) provides cryptographic security for authentication over an unsecured link.

The second technique is to map a user's password into a cryptographic key (e.g., a 56-bit DES key) by a one-way hash function. Such password-derived keys are called *passkeys*. The passkey is then used to secure a communication link between the user and a system that also knows the user password. It should be ensured that the entropy of the user's password is sufficiently large that an exhaustive search of the password space is not more efficient than an exhaustive search of the passkey space (i.e., guessing passwords is not easier than guessing 56-bit DES keys).

### 2.8.4 Challenge-Response Identification (Strong Authentication)

Challenge-response identification is also an important kind of authentication. The idea of cryptographic challenge-response protocols is that one entity (the claimant, or prover) "proves" its identity to another entity (the verifier) by demonstrating knowledge of a secret known to be associated with that entity, without revealing the secret itself to the verifier during the protocol. This is accomplished by answering a time-variant challenge, where the answer is determined by both the prover's secret and the challenge. The *challenge* is typically a random number chosen by one entity secretly at the outset of the protocol. Even if the communica-

tion line is monitored, the response from one execution of the identification protocol should not provide an adversary with useful information for a later authentication, as a later challenge will be different.

The protocols of challenge-response identification fall into three major classes. They are based on symmetric-key cryptosystems, public-key cryptosystems, and zero-knowledge proof systems [2.11], respectively.

### **Challenge-Response by Symmetric-Key Techniques**

Challenge-response mechanisms based on symmetric-key techniques require the claimant and the verifier to share a symmetric key. For closed systems with a small number of users, each pair of users may share a key in advance. In larger systems employing symmetric-key techniques, identification protocols often involve the use of a trusted online server. Each party shares a key with the trusted sever. The trusted sever effectively provides a common session key to two parties each time one requests authentication with the other.

The Kerberos protocol [2.11] and the Needham-Schroeder shared-key protocol [2.11] are good examples of authentication protocols that provide entity authentication based on symmetric encryption and involve the use of an online trusted third party. Kerberos protocol employs a client/server architecture and provides user-to-server authentication rather than host-to-host authentication. In this model, security and authentication are based on secret-key technology where every host on the network has its own secret key. It would clearly be unmanageable if every host had to know the keys of all other hosts, so a secure, trusted host somewhere on the network, known as a *key distribution center* (KDC), knows the keys for all of the hosts (or at least some of the hosts within a portion of the network, called a *realm*). In this way, when a new node is brought online, only the KDC and the new node need to be configured with the node's key (keys can be distributed physically or by some other secure means).

### **Challenge-Response by Public-Key Techniques**

In such identification protocols, a claimant demonstrates knowledge of its private key in one of the following two ways:

1. The claimant decrypts a challenge encrypted under its public key.
2. The claimant digitally signs a challenge.

Ideally, the public-key pair used in such mechanisms should not be used for other purposes, since combined usage may compromise security. A second caution is that the public-key system used should not be susceptible to chosen ciphertext

attacks, as an adversary may attempt to extract information by impersonating a verifier and choosing strategic rather than random challenges.

### **Challenge-Response by Zero-Knowledge Proof**

The verifier learns nothing about the fact being proved (except that it is correct) from the prover that the verifier could not already learn without the prover, even if the verifier does not follow the protocol (as long as the prover does). In a zero-knowledge proof, the verifier cannot even later prove the fact to anyone else. (Not all interactive proofs have this property.)

A typical round in a zero-knowledge proof consists of a “commitment” message from the prover, followed by a challenge from the verifier, and then a response to the challenge from the prover. The protocol may be repeated for many rounds. Based on the prover's responses in all the rounds, the verifier decides whether to accept or reject the proof.

There are few zero-knowledge and interactive proof protocols [2.17] used today as identification schemes. The *Fiat-Shamir protocol* is the first practical zero-knowledge protocol with cryptographic applications and is based on the difficulty of factoring. A more common variation of the Fiat-Shamir protocol is the Feige-Fiat-Shamir scheme. Guillou and Quisquater further improved Fiat-Shamir's protocol in terms of memory requirements and interaction (the number of rounds in the protocol).

### **2.8.5 Authentication Based on Certificate Authority**

The authentication technique based on *certificate authority (CA)* is similar to that of Kerberos. It realizes authentication using a mutually trusted third party. It employs public-key cryptosystems, and its realization is much simpler. The trusted third party here is the so-called CA. The CA is responsible for user identification and issues signed digital certificates for users. The digital certificate is called an X.509 certificate since it follows the format of the X.509 standard. A user possessing such a certificate can access those servers trusting CA. We will describe CA and X.509, in detail in the next Chapter.

When a user asks to access a server, they are asked to submit their digital certificate. The server decrypts and verifies the user's certificate. If the certificate is valid, the server then gets the user's public key. In subsequent communication with the user, the server can encrypt messages with the user's public key. The authentication mechanism based on an X.509 certificate is applicable to identification in an open-network environment. It has gained wide acceptance. Many network se-

curity programs, such as IPSec, SSL, SET, and S/MIME, all use this identification mechanism.

This authentication mechanism employs asymmetric cryptosystem so that the user's certificate and their private key are not transmitted in the network. Hence the security drawbacks of password-based authentication are effectively overcome. Even if the adversary intercepts a user's certificate, they still cannot decrypt the message delivered to the user since they do not know the user's private key.

There are already some authentication organizations on the Internet using the X.509 certificate mechanism. Verisign, US Postal Service, and CommerceNet are examples.

The certificate associates the unique user name with its public key. Whether or not this association is legal is beyond the X.509 standard. X.509 claims that whatever is concerned with semantics and trust relies on the *certification practice statement* (CPS) of CA. This will obviously result in differences in the methods and degree of strictness of identification. Thus, it is necessary to establish a uniform authentication system and related rules all over the world.

## 2.9 Summary

The promise of electronic commerce is one of the major factors that are contributing to the rapid growth of the Internet as a communications medium. With any commercial activity, it is important to consider the security implications of doing business. It will be especially important to support the use of cryptographic mechanisms for data protection, authentication, and privacy protection in electronic commerce. This chapter introduced the security of electronic commerce and the basics of cryptography. Particularly, it deals with the following themes:

- The essential requirements for carrying out secure electronic commerce.
- A basic introduction to cryptography, include secret-key cryptography, public-key cryptography, digital signature, Hash function, random number generators and authentication techniques.

## 2.10 References

- [2.1] D. Chaum, E. Heijst (1991) Group signatures. In: *Advances in cryptology – EUROCRYPT 91*, LNCS 547. Springer, Berlin Heidelberg New York, pp. 257–265.
- [2.2] D. Chaum, H. Antwerpen (1990) Undeniable signatures. In: *Advances in cryptology – CRYPTO 89*, LNCS 434. Springer, Berlin Heidelberg New York, pp. 212–216.
- [2.3] B. Chor, R.L. Rivest (1988) A knapsack-type public-key cryptosystem based on arithmetic in finite fields. *IEEE Trans Infor Theory* 34: 901–909.
- [2.4] J. Daemen, V. Rijmen (2002) *The design of Rijndael*. Springer, Berlin Heidelberg New York.
- [2.5] W. Diffie, M. Hellman (1976) New directions in cryptography. *IEEE Trans Infor Theory* 22: 644–654.
- [2.6] W. Ford, M. Baum (1997) *Secure electronic commerce: building the infrastructure for digital signatures encryption*. Prentice-Hall, Englewood Cliffs New York.
- [2.7] S. Garfinkel (1995) *PGP: pretty good privacy*. O’Reilly, Beijing Cambridge Farnham Koln Tokyo.
- [2.8] A. Kambil (draft) Trends in electronic commerce security background material for discussion on payments and settlements.  
<http://www.stern.nyu.edu/~akambil/teaching/cases/secure.pdf>.
- [2.9] N. Koblitz (1987) Elliptic curve cryptosystems. *Math Comput* 48: 203–209.
- [2.10] A. J. Menezes (1993) *Elliptic curve public key cryptography*. Kluwer, Boston Dordrecht London.
- [2.11] A. J. Menezes, P.C. Oorschot, S. A. Vanstone (1997) *Handbook of applied cryptography*. CRC Press, Boca Raton.
- [2.12] V. S. Miller (1986) Use of elliptic curves in cryptography. In: *Advances in cryptology – CRYPTO 85*, LNCS 218. Springer, Berlin Heidelberg New York, pp. 417–426.
- [2.13] R. L. Rivest, A. Shamir, L. M. Adleman (1978) A method for obtaining digital signatures and public-key cryptosystems. *Commun ACM* 21(2): 120–126.
- [2.14] G. J. Simmons (ed.) (1992) *Contemporary cryptology: the science of information integrity*. IEEE Press, New York.
- [2.15] SSH - tech corner - introduction to cryptography.  
<http://www.ssh.fi/tech/crypto/intro.html>.
- [2.16] D. R. Stinson (1995) *Cryptography: theory and practice*. CRC Press, Boca Raton.
- [2.17] W. Stallings (1999) *Cryptography and network security: principles and practice* (2nd ed.). Prentice-Hall, Upper Saddle River.
- [2.18] D. Chaum (1983): Blind signature for untraceable payments. In: *Advance in cryptology*. Plenum Press, New York, pp. 199–203.



## 3 Public-Key Infrastructure

Hui Li and Yumin Wang

National Key Laboratory of ISN  
Xidian University, Xi'an, China

### 3.1 Introduction

#### 3.1.1 What Is a PKI?

In its most simple form, a *Public-key infrastructure* (PKI) is a system for publishing the public-key values used in public-key cryptography. PKI is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on the Internet.

A PKI integrates digital certificates, public-key cryptography, and certificate authorities into a total, enterprise-wide network security architecture. A typical enterprise's PKI encompasses the issuance of digital certificates to individual users and servers; end-user enrollment software; integration with corporate certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.

#### 3.1.2 Why Do You Need PKI

PKI protects your information assets in several essential ways:

- **Authenticate identity.** Digital certificates issued as part of your PKI allow individual users, organizations, and web site operators to confidently validate the identity of each party in an Internet transaction.
- **Verify integrity.** A digital certificate ensures that the message or document the certificate "signs" has not been changed or corrupted in transit online.
- **Ensure privacy.** Digital certificates protect information from interception during Internet transmission.

- **Authorize access.** PKI digital certificates replace easily guessed and frequently lost user IDs and passwords to streamline intranet log-in security and reduce the MIS overhead.
- **Authorize transactions.** With PKI solutions, your enterprises can control access privileges for specified online transactions.
- **Support for non-repudiation.** Digital certificates validate their users' identities, making it nearly impossible to later repudiate a digitally "signed" transaction, such as a purchase made on a web site.

### 3.1.3 Certificates and Certificate Authorities (CAs)

A *certificate* is a collection of information that has been digitally signed by its issuer (see Fig. 3.1). Such certificates are distinguished by the kind of information they contain. An *identity certificate* is an electronic document used to identify an individual, a server, a company, or some other entity called the certificate *subject* and to associate that subject with a public key. A *credential certificate* describes non-entities, such as a permission or credential. Like a driver's license, a passport, or other commonly used personal IDs, a certificate provides generally recognized proof of a person's identity. Public-key cryptography uses certificates to address the problem of impersonation.

To get a driver's license, you typically apply to a government agency, such as the Department of Motor Vehicles, which verifies your identity, your ability to drive, your address, and other information before issuing the license. To get a student ID, you apply to a school or college, which performs different checks (such as whether you have paid your tuition) before issuing the ID. To get a library card, you may need to provide only your name and a utility bill with your address on it.

Certificates work much the same way as any of these familiar forms of identification. *Certificate authorities (CAs)* are entities that validate identities and issue certificates. They can be either independent third parties or organizations running their own certificate-issuing server software (such as Netscape Certificate Server). The methods used to validate an identity vary depending on the policies of a given CA, that is, just as the methods to validate other forms of identification vary depending on who is issuing the ID and the purpose for which it will be used. In general, before issuing a certificate, the CA must use its published verification procedures for that type of certificate to ensure that an entity requesting a certificate is in fact who it claims to be.

The certificate issued by the CA binds a particular public key to the name of the entity the certificate identifies (such as the name of an employee or a server). Certificates help prevent the use of fake public keys for impersonation. Only the public key certified by the certificate will work with the corresponding private key possessed by the entity identified by the certificate.

In addition to a public key, a certificate always includes the name of the entity it identifies, an expiration date, the name of the CA that issued the certificate, a serial number, and other information. Most importantly, a certificate always includes the digital signature of the issuing CA. The CA's digital signature allows the certificate to function as a "letter of introduction" for users who know and trust the CA but don't know the entity identified by the certificate.

A certificate *user* is an entity who relies upon the information contained in a certificate. The certificate user trusts the issuing authority to issue true certificates, that is, certificates that truly identify the subject and its public key (in the case of identity certificates), or that truly describe a subject's credentials (in the case of credential certificates).

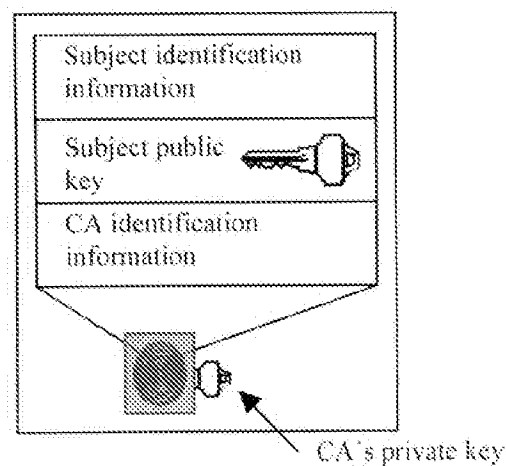


Fig. 3.1 A basic certificate

To help illustrate these concepts, we present an example using identity certificates. Imagine that Alice wishes to securely communicate with Bob using a public key cryptosystem. Alice needs to know the value of Bob's public encrypting key. Without a PKI, Alice must have direct knowledge of that key, i.e., Bob must communicate it to her via a secure channel.

With a PKI, Alice only needs to have direct knowledge of a CA's public signing key. The CA would issue an identity certificate for each of Bob's public encrypting keys. Then if Alice wishes to communicate with Bob, she can use the appropriate certificate to obtain the correct public key value. In this case, Alice is the certificate user while Bob is the subjects of certificate. See Fig. 3.2.

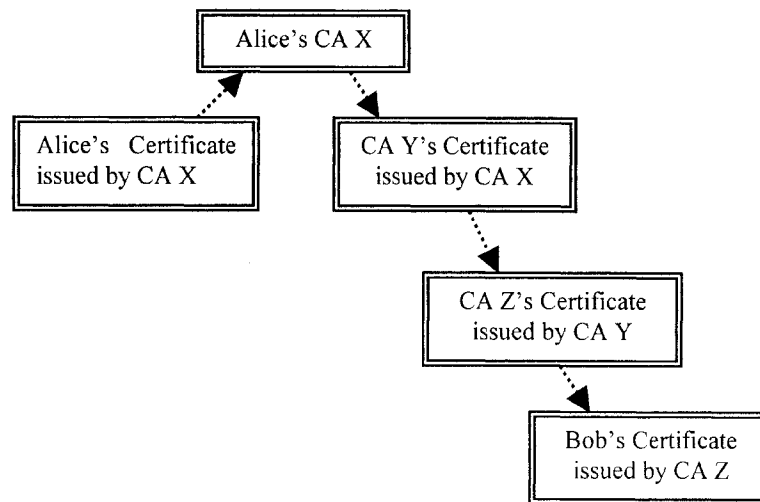


Fig. 3.2 A certification path from Alice to Bob

### 3.1.4 CA Arrangements

#### Certificate Hierarchies

In large organizations, it may be appropriate to delegate the responsibility for issuing certificates to several different certificate authorities. For example, the number of certificates required may be too large for a single CA to maintain; different organizational units may have different policy requirements; or it may be important for a CA to be physically located in the same geographic area as the people to whom it is issuing certificates.

It's possible to delegate certificate-issuing responsibilities to subordinate CAs. The X.509 standard includes a model for setting up a hierarchy of CAs like that shown in Fig. 3.3.

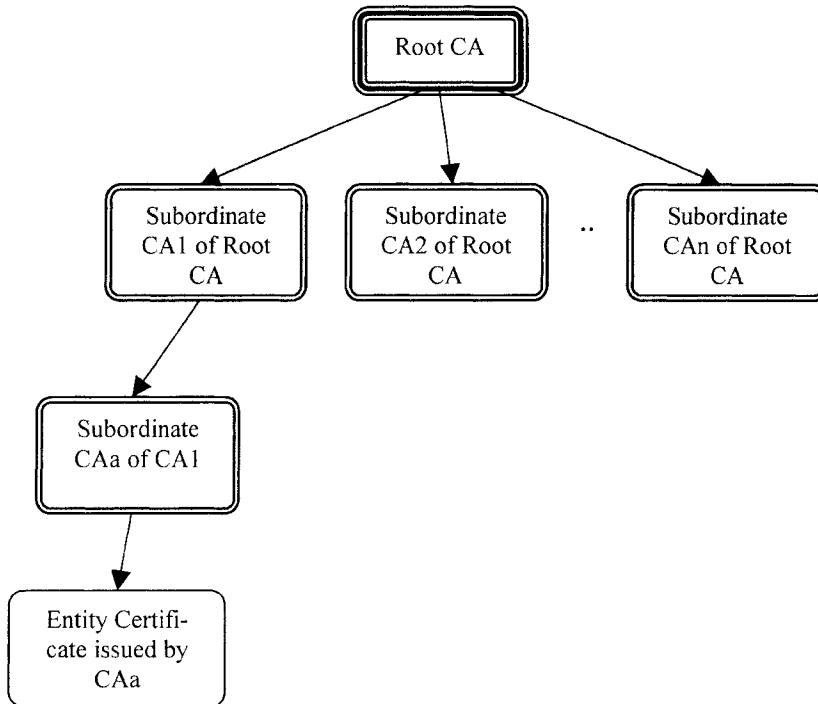


Fig. 3.3 Example of a hierarchy of certificate authorities

In this model, the root CA is at the top of the hierarchy. The root CA's certificate is a *self-signed certificate*, that is, the certificate is digitally signed by the same entity (the root CA) that the certificate identifies. The CAs that are directly subordinate to the root CA have CA certificates signed by the root CA. CAs under the subordinate CAs in the hierarchy have their CA certificates signed by the higher-level subordinate CAs.

Organizations have a great deal of flexibility in terms of the way they set up their CA hierarchies. Fig. 3.3 shows just one example; many other arrangements are possible.

### Certificate Chains

CA hierarchies are reflected in certificate chains. A *certificate chain* is series of certificates issued by successive CAs. Fig. 3.4 shows a certificate chain leading from a certificate that identifies some entity through two subordinate CA certi-

ates to the CA certificate for the root CA (based on the CA hierarchy shown in Fig. 3.3).

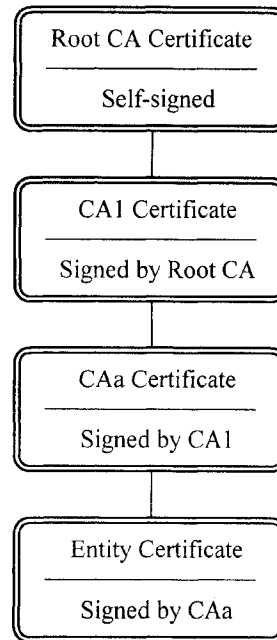


Fig. 3.4 Example of a certificate chain

A certificate chain traces a path of certificates from a branch in the hierarchy to the root of the hierarchy. In a certificate chain, the following occur:

- Each certificate is followed by the certificate of its issuer.
- Each certificate contains the name (DN) of that certificate's issuer, which is the same as the subject name of the next certificate in the chain.

In Fig. 3.4, the CAa certificate contains the DN of the CA1, that issued that certificate. CA1's DN is also the subject name of the next certificate in the chain.

- Each certificate is signed with the private key of its issuer. The signature can be verified with the public key in the issuer's certificate, which is the next certificate in the chain.

In Fig. 3.4, the public key in the certificate for the CA1 can be used to verify the CA1's digital signature on the certificate for the CAa.

### 3.1.5 Validation

The other basic PKI operation is certificate validation. The information in a certificate can change over time. A certificate user needs to be sure that the certificate's data is true, that is, the user needs to *validate* the certificate. There are two basic methods of certificate validation. A PKI can use either or both methods.

- The user can ask the CA directly about a certificate's validity every time it is used. This is known as *online* validation.
- The CA can include a *validity period* in the certificate – a pair of dates that define a range during which the information in the certificate can be considered as valid. This is known as *offline* validation.

#### Verify a Certificate Chain

Certificate chain verification is the process of making sure a given certificate chain is well-formed, valid, properly signed, and trustworthy. A PKI usually uses the following procedure for forming and verifying a certificate chain, starting with the certificate being presented for authentication.

1. The certificate validity period is checked against the current time provided by the verifier's system clock.
2. The issuer's certificate is located. The source can be either the verifier's local certificate database (on that client or server) or the certificate chain provided by the subject (for example, over an SSL connection).
3. The certificate signature is verified using the public key in the issuer's certificate.
4. If the issuer's certificate is trusted by the verifier in the verifier's certificate database, verification stops successfully here. Otherwise, the issuer's certificate is checked to make sure it contains the appropriate subordinate CA, and chain verification returns to step 1 to start again, but with this new certificate. Fig. 3.5 presents an example of this process.

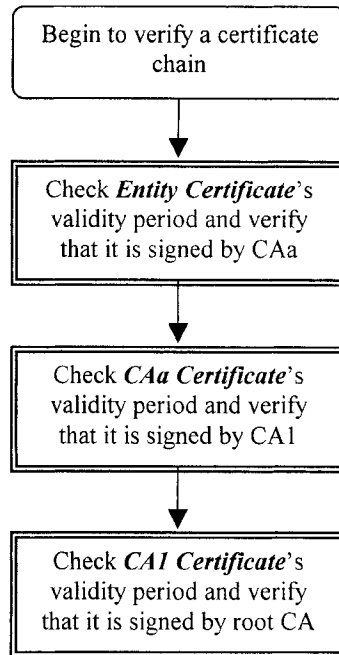


Fig. 3.5 Verifying a certificate chain all the way to the root CA

### Certificate Revocation Lists (CRLs)

Closely related to the validation method is certificate *revocation*. Certificate revocation is the process of letting users know when the information in a certificate becomes unexpectedly invalid. This can occur when a subject's private key becomes compromised, or, more benignly, when a certificate's identifying information changes (e.g. the subject gets a new telephone number).

If a certificate is validated online with the CA every time it is used, then the revocation problem becomes trivial, as the CA can simply state that the certificate is no longer valid. However, when validity periods are employed, the certificate revocation method becomes critical (especially in the case of private-key compromise).

In the absence of online approaches, the most common revocation method uses *certificate revocation lists* (CRLs). A CRL is a list of revoked certificates that is signed and periodically issued by a CA. It is essential that the user check the latest



CRL during validation to make sure that a certificate she is about to use has not been revoked.

One of the chief concerns with the CRL approach is what happens between the time when a CA receives notification that a certificate should be revoked and when the CA publishes its next CRL. Since the revoked certificate will only appear on the next CRL, any user checking the current CRL will not know of its revocation and will assume that the certificate is still valid. We call this the *CRL time-granularity problem*.

Another concern is the size of the CRL. A CA can be expected to certify thousands, or even hundreds of thousands, of subjects. While the rate of revocations for a given population is generally unpredictable, the CRLs for such CAs can be expected to grow very large. When a CRL is too large it can be difficult to retrieve by users, whose access to the CA may have limited bandwidth. Also, since CRLs are signed, their signatures need to be verified before the CRL can be used, and the time required to verify the signature on a large CRL and process its entries can become significant.

These problems have led to several refinements of the CRL approach. One is to issue separate CRLs for different revocation reasons and/or for different certificate subjects. For example, the CA could issue one CRL for routine revocations (e.g., a change in a certificate subject's identifying information) and another CRL for revocations due to a security compromise. Similarly, a CA could issue one CRL for its end-user subjects and another for the other CAs it may certify. These measures have the effect of partitioning a large CRL into pieces that can be selectively digested. For example, a user might not be very worried about routine revocations and so would only need to check the security-compromise CRL. Also, when processing a certification path the user need only check the CA CRLs (until reaching the end of the path).

While these steps help reduce CRL sizes, they do little to alleviate the CRL time-granularity problem. Another measure has been proposed to address that problem: *delta-CRLs*. A delta-CRL is simply a (CA-signed) list of CRL changes that have occurred since the last full CRL was issued. Delta-CRLs allow revocation notifications to be issued more frequently, and so reduce the probability that a revoked certificate will be falsely validated. Delta-CRLs also help with the CRL size problem. A certificate validating system could start with a full CRL, and then need only process delta-CRLs as they are issued, updating its own copy of the full CRL.

### 3.1.6 Authentication

Authentication is the process of using a PKI. When a CA certifies an entity and a user then validates that certification, the entity is said to have been *authenticated*.

A certificate can contain entity or nonentity information. When a certificate identifies an entity, it is called an *identity certificate*. Authenticating an identity certificate is called *identity authentication*.

Certificates that contain nonentity information, such as a permission or credential, are called *credential certificates*. Credential certificates identify things such as permissions (e.g., an access computer xyz), credentials (e.g., as a certified stock broker), or other attributes (e.g., as VP Marketing for “ABC Inc.”). A credential certificate may or may not identify the entity to which the credential is attached. We call authenticating a credential certificate *credential authentication*.

In the context of network interactions, authentication involves the confident identification of one party by another party. Authentication over networks can take many forms. Certificates are one way of supporting authentication.

Network interactions typically take place between a client, such as browser software running on a personal computer, and a server, such as the software and hardware used to host a web site. *Client authentication* refers to the confident identification of a client by a server (that is, identification of the person assumed to be using the client software). *Server authentication* refers to the confident identification of a server by a client (that is, identification of the organization assumed to be responsible for the server at a particular network address).

Client and server authentication are not the only forms of authentication that certificates support. For example, the digital signature on an email message, combined with the certificate that identifies the sender, provide strong evidence that the person identified by that certificate did indeed send that message. Similarly, a digital signature on an HTML form, combined with a certificate that identifies the signer, can provide evidence, after the fact, that the person identified by that certificate did agree to the contents of the form. In addition to authentication, the digital signature in both cases ensures a degree of non-repudiation, that is, a digital signature makes it difficult for the signer to claim later not to have sent the email or the form.

### 3.1.7 Limitations of PKI Authentication

Whenever authentication is performed using the PKI, whether online or offline, it is called *in-band authentication*. Authentication performed using more traditional methods, such as over the telephone or physically meeting someone, is called *out-of-band authentication*. The goal of every PKI is to minimize the need for out-of-band authentication.

It is unlikely that out-of-band authentication can ever be completely eliminated. At the very least, a person wishing to use a PKI needs to first have their identity and/or credentials verified by their CA. This initial verification cannot be per-

formed using the PKI, since there is no other CA to vouch for the person's identity/credentials. Thus the bootstrapping process requires out-of-band authentication. Also, different PKIs require different degrees of out-of-band authentication as identity and credential information changes over time and needs to be updated.

The extent to which out-of-band authentication is required in a PKI is partly a result of how much the PKI's designers want to provide *irrefutability*. A signature made by Alice is said to be irrefutable if Alice can not, at a later date, deny that she did in fact make the signature. If the PKI is to be used as the foundation of an electronic replacement for paper-based signatures, then irrefutability is an important consideration. In general, the more out-of-band contact Alice has with her CA, the less she will be able to engage in such fraud.

### 3.1.8 Registration Authorities

Interactions between entities identified by certificates (sometimes called *end entities*) and CAs are an essential part of certificate management. These interactions include operations, such as registration for certification, certificate retrieval, certificate renewal, certificate revocation, and key backup and recovery. In general, a CA must be able to authenticate the identities of end entities before responding to the requests. In addition, some requests need to be approved by authorized administrators or managers before being serviced.

As previously discussed, the means used by different CAs to verify an identity before issuing a certificate can vary widely, depending on the organization and the purpose for which the certificate will be used. To provide maximum operational flexibility, interactions with end entities can be separated from the other functions of a CA and handled by a separate service called a *registration authority* (RA).

An RA acts as a front end to a CA by receiving end entity requests, authenticating them, and forwarding them to the CA. After receiving a response from the CA, the RA notifies the end entity of the results. RAs can be helpful in scaling a PKI across different departments, geographical areas, or other operational units with varying policies and authentication requirements.

### 3.1.9 Certificates and the LDAP Directory

The lightweight directory access protocol (LDAP) for accessing directory services supports great flexibility in the management of certificates within an organization. System administrators can store much of the information required to manage certificates in an LDAP-compliant directory. For example, a CA can use information in a directory to pre-populate a certificate with a new employee's legal name and other information. The CA can leverage directory information in other ways to is-

sue certificates one at a time or in bulk, using a range of different identification techniques depending on the security policies of a given organization. Other routine management tasks, such as key management and renewing and revoking, can be partially or fully automated with the aid of the directory.

Information stored in the directory can also be used with certificates to control access to various network resources by different users or groups. Issuing certificates and other certificate management tasks can thus be an integral part of user and group management.

### **3.1.10 Key Management**

Before a certificate can be issued, the public key it contains and the corresponding private key must be generated. Sometimes it may be useful to issue a single person one certificate and key pair for signing operations, and another certificate and key pair for encryption operations. Separate signing and encryption certificates make it possible to keep the private signing key on the local machine only, thus providing maximum non-repudiation, and to back up the private encryption key in some central location where it can be retrieved in case the user loses the original key or leaves the company.

Keys can be generated by client software or generated centrally by the CA and distributed to users via an LDAP directory. There are tradeoffs involved in choosing between local and centralized key generation. For example, local key generation provides maximum non-repudiation, but may involve more participation by the user in the issuing process. Flexible key management capabilities are essential for most organizations.

## **3.2 X.509**

### **3.2.1 Introduction**

X.509 [3.65] is the authentication framework designed to support X.500 directory services [3.64]. Both X.509 and X.500 are part of the X series of international standards proposed by the ISO and ITU. The X.500 standard is designed to provide directory services on large computer networks. X.509 provides a PKI framework for authenticating X.500 services.

The first version of X.509 appeared in 1988, making it the oldest proposal for a worldwide PKI. This, coupled with its ISO/ITU origin, has made X.509 the most

widely adapted PKI. There are at least a dozen companies worldwide that produce X.509-based products, and that number is growing. Visa and MasterCard have adapted X.509 as the basis for their secure electronic transaction standard (SET) [3.55]. Netscape's famous World Wide Web software also uses X.509. And there are numerous X.509-based products available from companies, such as Entrust and TimeStep that support corporate intranets. Efforts are currently underway to design an X.509-based PKI that will support a global network such as the Internet. Along with PGP [3.67], X.509 is the only PKI system that has yet to be put into practical use.

### 3.2.2 The X.509 Standard

#### X.500

A full understanding of X.509 PKIs requires some basic knowledge of the X.500 directory that X.509 was originally designed for. The X.500 directory [3.64] is very similar to a telephone directory where, given a person's name, one can find auxiliary information about that person. However, X.500 provides more than just a name, address, and phone number. An entry in an X.500 directory can contain a host of attributes, such as the name of the organization the person works for, their job title and their email address, to name a few. An X.500 directory entry can represent any real-world entity, not just people but also computers, printers, companies, governments, and nations. The entry can also contain the certificate specifying the entity's public key.

#### Distinguished Name

To support looking up entries in the directory, each entry is assigned a globally unique name, called a *distinguished name* or DN. To help ensure their uniqueness, these names are assigned in a very specific fashion. The X.500 directory is arranged in a hierarchical fashion, call the *Directory Information Tree* or DIT (see Fig. 3.6).

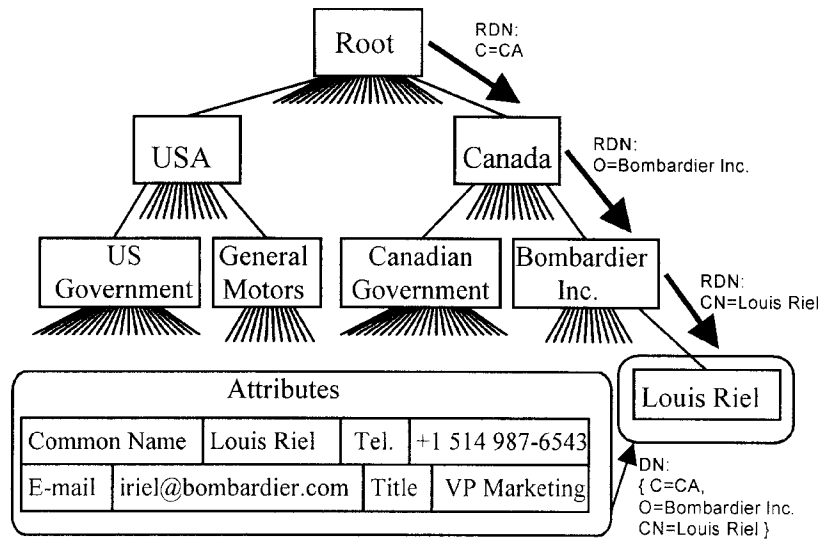


Fig. 3.6 The X.500 directory information tree

Each node, or *vertex*, in the tree has one parent (except the root vertex) and any number of children. Each vertex, except the root, is assigned a *relative distinguished name* (RDN) that is unique among all the vertex's siblings. The RDNs of each of the vertex's ancestors are concatenated with the vertex's own RDN to form the entry's DN. Fig. 3.6 illustrates this process. Under the root vertex there is an entry for each country in the world. These entries are assigned an RDN that is the country's unique two-letter code assigned to it by the ISO. Beneath each country's vertex are entries for all of the country's organizations, such as its government, its states or provinces, and federally-chartered companies. Each of these is assigned a unique RDN that is the name of the organization. Finally, each organization creates entries for all of its employees, and for other entities the organization might control. Each of these is also assigned a unique RDN. In our example, Mr. Louis Riel works for Bombardier, a Canadian company. Bombardier assigns an RDN to Mr. Riel, that is simply his name (specified as his common name, abbreviated as CN in the figure). Bombardier was itself assigned an RDN, Organization = Bombardier by Canada, designating it as the organization named Bombardier, and Canada's RDN is its two-letter country code, Country = CA. Mr. Riel's DN is thus the concatenation of these RDNs, starting from the root: Country = CA, Organization = Bombardier, CommonName = Louis Riel.

### X.509 Version 2 certificate

X.509 was created to support the authentication of the entries in an X.500 directory. The latest version, the third, has evolved beyond its X.500 roots. Currently, version 3 is the official standard. We will first describe X.509v2, before moving on to the extensions added under version 3.

The X.509v2 certificate is illustrated in Fig. 3.7. It contains the following fields.

- Version: The X.509 version that the certificate conforms to.
- Serial number: A unique number assigned to the certificate by its issuing CA.
- CA signature algorithm: An identifier for the algorithm used by the CA to sign the certificate. Identifiers are further discussed below under Object Registration.
- Issuer name: The X.500 name of the issuing CA.
- Validity period: A pair of dates/times between which the certificate is considered valid.
- Subject name: The X.500 name of the entity who holds the private key corresponding to the public key being certified.
- Subject public key information: The value of the subject's public key along with an identifier of the algorithm with which the key is intended to be used.
- Issuer unique identifier (optional, version 2 only): A bit string used to make the X.500 name of the issuing CA unambiguous. It is possible for an X.500 name to be assigned to a particular entity, then de-assigned, then re-assigned to a new entity.<sup>1</sup> The unique identifier fields address this concern. These fields are not widely used, as they have turned out to be difficult to manage and are ignored or omitted in most implementations. The preferred method used to address this problem is to design the RDNs in such a way as to ensure that they are *never* reused. For example, rather than use just the CommonName attribute, a better form of RDN might use both the CommonName and an EmployeeNumber.
- Subject unique identifier (optional, version 2 only): A bit string used to make the X.500 name of the subject unambiguous.

---

<sup>1</sup> For example, in Fig. 3.6, if Mr. Riel changes companies, his DN, in particular the Organization=Bombardier component, is no longer valid and so is de-assigned. Later, if another person named Louis Riel comes to work for Bombardier, he would be assigned the same DN as the first Louis Riel.

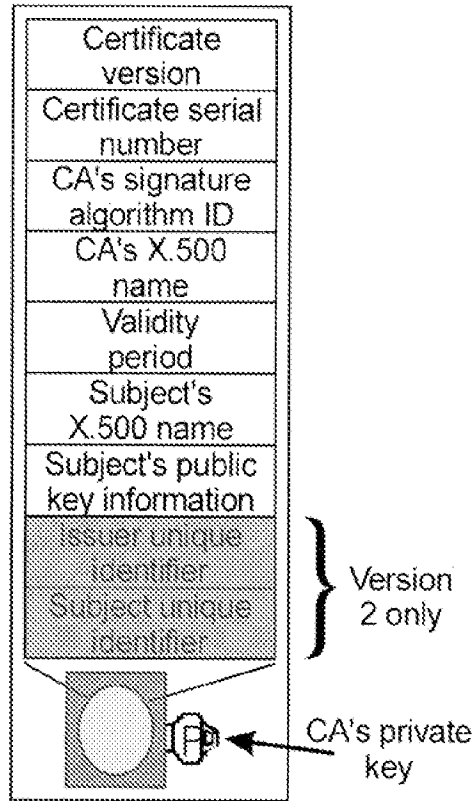


Fig. 3.7 The X.509 version 2 certificate

Because of X.509's close ties with X.500, its CAs are usually arranged in a hierarchy that closely follows the X.500 DIT.

X.509, and X.500, were originally designed in the mid-1980's, before the current explosive growth of the Internet. They were therefore designed to operate in an offline environment, where computers are only intermittently connected to each other. X.509 thus employs CRLs. Versions 1 and 2 of X.509 use very simple CRLs that do not address size issues and the time-granularity problem. Version 3 makes several attempts to solve these problems, with varying success. Fig. 3.8 illustrates the CRL format used in X.509 versions 1 and 2.



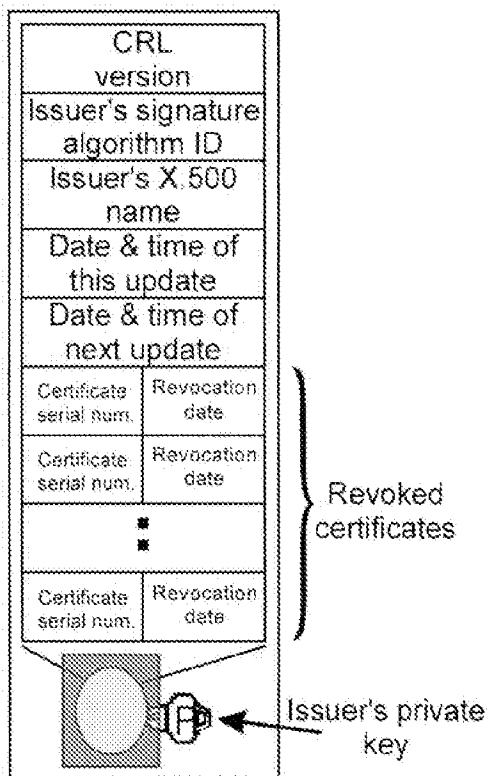


Fig. 3.8 X.509 version 1 CRL format

**X.509 Version 3**

Version 3 introduced significant changes to the X.509 standard. The fundamental change was to make the certificate and CRL formats extensible. X.509 implementers can now define certificate contents as they see fit. Also, a number of standard extensions were defined to provide key and policy information, subject and issuer attributes, certification path constraints, and enhanced CRL functionality. These extensions are fully described in [3.10] and elsewhere. We concentrate here on those extensions which affect the basic PKI characteristics of X.509.

### Version 3 Certificate Extensions

***Certificate policies and policy mapping.*** X.509v3 gives CAs the ability to include with the certificate a list of policies that were followed in creating the certificate. These policies are intended to help users decide if a certificate is suitable for a particular purpose. For example, a policy might indicate that a certified key can be used for casual email messages but not for financial transactions. In general, a certificate policy indicates such things as CA security procedures, subject identification measures, legal disclaimers or provisions, and others. Policy mapping allows a CA to indicate whether one of its policies is equivalent to another CA's policy.

***Alternative names.*** An X.509v3 certificate can contain one or more alternative names for the subject or issuer. This allows X.509 to operate without an underlying X.500 directory. Examples of alternative names include email addresses and World Wide Web universal resource locators. Implementers can also define their own alternative name forms. Alternative names can also be used to identify the issuer of a CRL.

***Subject directory attributes.*** This extension allows any of the subject's X.500 directory entry attribute values to be included in the certificate. This allows the certificate to carry additional identifying information beyond the subject's name(s).

***Certification path constraints.*** These extensions allow CAs to link up their infrastructures in meaningful ways. A CA can restrict the kinds of certification paths that can grow from certificates it issues for other CAs. The CA can state whether or not a certificate's subject is in fact a CA (to prevent an end user from fraudulently acting as a CA). The CA can also constrict paths growing from the certificate to certificates issued in a particular name space (e.g., within a given Internet domain) and/or to certificates that follow a specific set of certification policies. This is an important extension because it allows CAs to employ a *progressive-constraint* trust model that prevents the formation of infinite certification paths. The concept is illustrated in Fig. 3.9. User a uses D as her certification authority, so she places complete trust in D. D has certified another certification authority, E, for example only trusting E to issue certificates for other CAs (perhaps E performs some kind of national CA registration). Constraint X would then state that D only trusts E to certify other certification authorities.

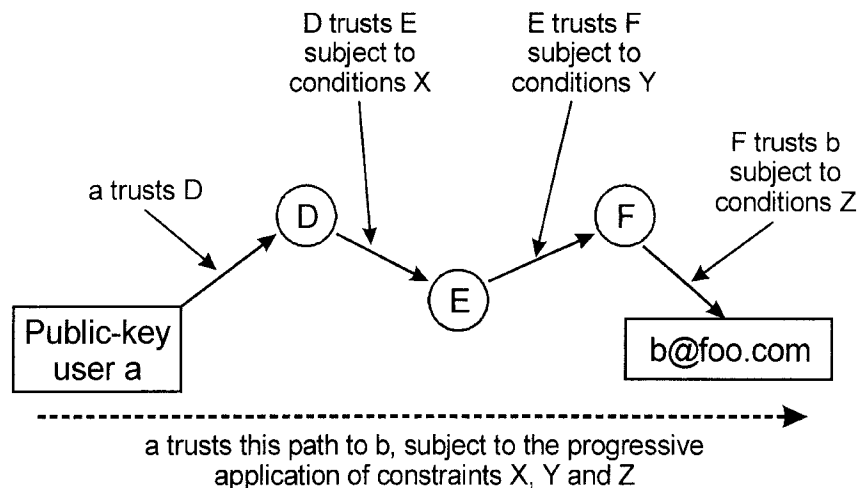


Fig. 3.9 A progressive-constrained trust chain

E has issued a certificate for certification authority F stating that it only trusts F to issue certificates for end users in the domain foo.com. So constraint Y would state that E trusts certificates issued by F only if they certify an end user *and* that user's name is in the foo.com domain. Finally, F issues a certificate for user b, but only trusts b for casual email (as opposed to, say, making financial commitments on F's behalf). So constraint Z states that the certificate issued for b by F should only be used for casual email.

In this way the unlimited trust that a places in D becomes increasingly constrained as the certification path grows. When a obtains a certificate for b she knows that she should only use it for casual email, and she has greater confidence in the strength of the authentication than with, say, PGP's web of trust because she can see how trust has been restricted along the certification path. Given these constraints, she would not accept a certificate issued by E for b (or any other user), nor would she accept any certificates from any certification authority certified by F. If CAs define the tightest practical conditions when they certify other CAs, then as a certification path grows it becomes progressively more constrained until it can grow no longer.

### Version 3 CRL Extensions

**CRL number and reason codes.** Each CRL issued for a given certificate population is assigned a number from a monotonically increasing sequence. This allows users to determine if a CRL was missed. Also, each certificate in a CRL can now

have a revocation reason attached to its CRL entry. These two extensions allow for the more sophisticated CRL extensions described below.

**CRL distribution points.** This extension helps reduce the sizes of CRLs processed by a CA's users. Rather than forcing users to accept the full CRL, the CA can partition the CRL in some way, and issue each partition from a different distribution point. For example, a corporate CA might issue a different CRL for each division of the company. Then when a user wants to verify a certificate for someone from a particular division, they need only check that division's CRL rather than the full CRL. Another way of partitioning the CRL is according to revocation reason. Routine revocations, for example, those due to a name change, can be placed on a different CRL than revocations due to a security compromise. The compromise list can then be updated and checked more frequently without having to also process all the routine revocations that might occur.

**Delta-CRLs.** This extension provides another method of reducing CRL sizes. Rather than issue a full CRL (or a full partition of a CRL), the CA can simply issue a list of the changes that have occurred since the last time a full CRL was issued. Users that maintain their own CRL database can use a delta-CRL to keep their copies updated without having to download and process all the entries of a full CRL, saving bandwidth and computing time.

**Indirect CRLs.** This extension allows a CRL to be issued from an entity other than the CA that issued its certificates. This allows for CRL clearing houses that would gather the CRLs from multiple CAs and provide one distribution point for them all.

All of these CRL extensions still do not overcome the fundamental time-granularity problem. Even with partitioned CRLs and frequent delta-CRL issuance, there is still a window of opportunity for a compromised certificate to be used. The X.509v3 framework can be used for online operation, avoiding the need for CRLs altogether. PKIX defines a *online certificate status protocol* [3.48] to do this work.

### **Object Registration**

The extensibility of X.509v3 gives it a tremendous amount of flexibility. However, the way in which that extensibility is provided hampers the widespread application of user-defined extensions for a global PKI.

Every time X.509 needs to identify some object, such as a signature algorithm, certification policy, user-defined alternative name, or a user-defined extension, it uses an internationally defined *object identifier* (OID) mechanism. An OID is a numeric value, composed of a sequence of integers, that is unique with respect to all other OIDs.

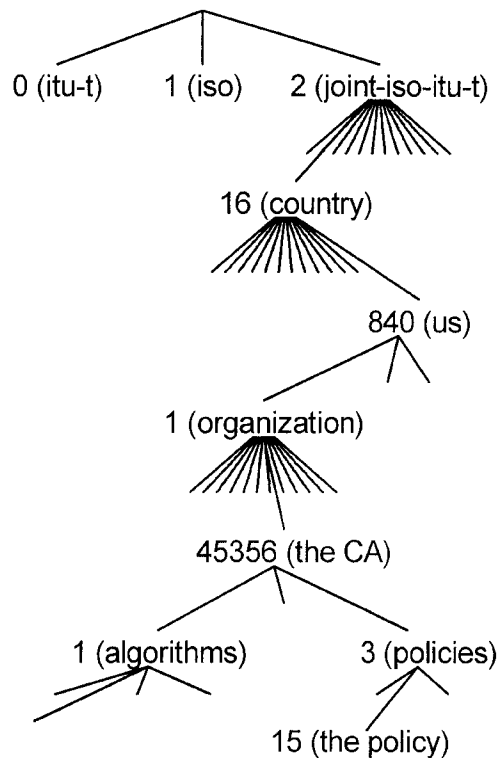


Fig. 3.10 Object registration example

The OIDs are assigned following a hierarchical structure of value-assigning authorities [3.10, 3.64, 3.66]. Essentially, any company or organization can become a value-assigning authority. The company is itself assigned a value that serves as a prefix for all the values that it defines. Take, for example, the OID pictured in Fig. 3.10. Imagine a CA operating in the United States. The CA would be assigned an OID, say 2-16-840-1-45356.<sup>2</sup> This OID would then be the prefix used for the OIDs of any objects that the CA cares to register. The CA might want to register a

<sup>2</sup> The numbers only have meaning within the hierarchy. The leading 2 indicates the branch of the hierarchy administered jointly by the ISO and ITU. The 16 is the number assigned to the branch used by national registration authorities. 840 is the country code for the U.S., whose national registration authority (ANSI) uses 1 as the prefix for all the organizations it registers. The 45356 is simply a number assigned to the CA by ANSI.

particular certification policy to which it has assigned a number, say 15, beneath the policy's branch of its hierarchy (branch number 3, for example). Then the CA's policy could be identified as object number 2-16-840-1-45356-3-15.

This system works well for assigning numbers to objects, and it is used extensively in X.509. For example, if the CA in Fig. 3.10 were to use its policy in a certificate, that policy would be identified solely by its OID. Difficulty arises, however, when OIDs are used without prior agreement as to their meaning. If the CA in our example wants to use their policy in their certificates, they have to ensure that the meaning of the OID identifying their policy is known *a priori* by any entity wishing to use the certificate. Otherwise, when an ignorant entity encounters the value 2-16-840-1-45356-3-15 it will have no idea how to interpret the policy.

Confusion can also arise when the same object is assigned multiple OIDs. For example, imagine that two CAs have each assigned an OID to a particular signature algorithm, such as SHA-with-RSA. As long as the CAs and their users don't interact, there will be no problems. However, if a user from one CA tries to use the other CA's certificate, they won't recognize the second CA's OID for SHA-with-RSA, and might assume that they can't verify the signatures of the certificate's subject even though they may be perfectly capable of doing so. The problem is compounded if the two CAs ever try to link their infrastructures. Then the CAs must either let all their users know that the two OIDs are equivalent, or one CA (or both) has to change its OID and communicate that change to all its users.

The OID problem prevents X.509's extensibility from being used freely on a large scale, since whoever creates a new extension must ensure that the relevant OIDs are known by all parties concerned. There is at present no systematic method for determining the meaning of an OID. They are neither regularly published, nor are they reliably listed in a central registry. The only way you can find out the meaning of an OID is to have the OID's creator tell it to you.

### 3.2.3 X.509 on the Internet

#### **Privacy Enhanced Mail**

Privacy enhanced mail (PEM) was proposed in early 1993 as an Internet standard for cryptography-enhanced email (see [3.34-3.37]). The intention was to endow Internet email with confidentiality, authentication, message integrity assurance, and non-repudiation of origin, using public-key cryptography. To this end, [3.35] proposed an Internet PKI to support PEM. The standard never caught on in the Internet community for various reasons, one of which was that its proposed PKI model proved to be a poor fit to the Internet's peer-based structure.

## **PKIX**

The PKIX working group (WG) was established in the fall of 1995 with the intent of developing Internet standards needed to support an X.509-based PKI. Several informational and standards track documents in support of the original goals of the WG have been approved by the IESG. The first of these standards, RFC 2459 [3.43], profiles the X.509 version 3 certificates and version 2 CRLs for use in the Internet. The certificate management protocol (CMP) (RFC 2510) [3.44], the online certificate status protocol (OCSP) (RFC 2560) [3.48], and the certificate management request format (CRMF) (RFC 2511) [3.45] have been approved, as have profiles for the use of LDAP v2 for certificate and CRL storage (RFC 2587) [3.50] and the use of FTP and HTTP for transport of PKI operations (RFC 2585) [3.49]. RFC 2527 [3.46], an informational RFC on guidelines for certificate policies and practices also has been published, and the IESG has approved publication of an information RFC on use of KEA (RFC 2528) [3.47] and is expected to do the same for ECDSA. Work continues on a second certificate management protocol, CMC, closely aligned with the PKCS publications and with the cryptographic message syntax (CMS) developed for S/MIME. A roadmap, providing a guide to the growing set of PKIX document, is also being developed as an informational RFC.

The working group is now embarking on additional standards work to develop protocols that are either integral to PKI management, or that are otherwise closely related to PKI use. Work is ongoing on alternative certificate revocation methods. There also is work defining conventions for certificate name forms and extension usage for “qualified certificates,” certificates designed for use in (legally binding) non-repudiation contexts. Finally, work is underway on protocols for time stamping and data certification. These protocols are designed primarily to support non-repudiation, making use of certificates and CRLs, and are so tightly bound to PKI use that they warrant coverage under this working group.

### **3.3 Credential-Based PKI Systems**

Much recent work has focused on moving away from identity-based PKIs to a more general system based on attributes or credentials. At present, there are two main proposals for this kind of system: the simple distributed security infrastructure (SDSI), and the simple public key infrastructure (SPKI).

#### **3.3.1 Simple Distributed Security Infrastructure (SDSI)**

SDSI was created by Ron Rivest and Butler Lampson and is described in [3.54]. SDSI is designed to facilitate the construction of secure systems and provides

simple, clear terminology for defining access-control lists and security policies. It is also an attempt to move away from identity-based certification and towards a system based on roles and credentials.

The SDSI system is key-centric. Rather than attach a public key to an identity, SDSI entities are the keys themselves. Specifically, SDSI calls its entities “principals” and defines them to be digital signature verification keys. The idea is that the key is a proxy for the individual who controls its associated private key. Thus SDSI principals are public keys that can make declarations by issuing verifiable signed statements.

### 3.3.2 SDSI Certificates

Those signed statements come mainly in the form of certificates. SDSI provides for three types of certificates, and any principal can create any kind of certificate. In no particular order, the three certificate types are:

- Identity certificates
- Group-membership certificates
- Name-binding certificates

SDSI identity certificates bind some identifying information to a principal. The main goal of a SDSI identity certificate is to allow a human reader to identify the individual behind a principal. As such, the certificates are designed to be human-friendly, usually containing some free-form text and perhaps a photograph or other information. Machine-readable tags, such as OIDs, are not used, because SDSI’s designers believe that determining the identity behind a principal will almost always involve a human anyway.

Identity certificates play a relatively small role in the SDSI system. More important are group-membership certificates, which assert that a principal does or does not belong to some group (more on SDSI groups below), and name-binding certificates, which bind a name to some value (typically, but not necessarily, a principal).

### 3.3.3 SDSI Names

When a principal creates a certificate binding a name to some value, that name is said to exist in the principal’s *local name space*. Each principal can create their own local names which they can use to refer to other principals. The names are arbitrarily chosen – there is no naming system to follow, and no attempt is made make names that are “globally” unique across all local names spaces. Thus some



principal that Alice has named bob may be completely different from the principal that Carl calls bob.

SDSI provides a simple method to *link* local name spaces together. If Alice has named a principal Bob, and Bob has named another principal Jim, then Alice can refer to that second principal as Bob's Jim. Alice can refer to any of bob's principals in this way, and the chain can be extended indefinitely, for example, as in bob's jim's mother's doctor. Names can also be "symbolically" defined. For example, Alice's local name bob can denote company's Bob-Smith. If the principal that Alice calls company changes the principal it calls Bob-Smith, then the principal that she calls bob changes as well.

SDSI achieves this name linking because it has an online orientation. Principals that issue certificates are assumed to be able to provide an on-line Internet server to distribute those certificates upon request. Thus for Alice to find the actual principal behind the name bob's jim, she simply connects to bob's server and requests the name-binding certificate that defines the name jim.

SDSI also provides for multiple global name spaces. These are the name spaces defined by a small set of *distinguished root* principals. These principals have special reserved names (that end with !!), which are bound to the *same* principal in *every* name space. SDSI does not describe how this is achieved in any detail. However, it does give SDSI the power to access "standard" name spaces, for example VeriSign!!'s Microsoft's CEO or DNS!!'s com's microsoft's "Bill Gates". Here, the name VeriSign!! evaluates to the *same* principal in *all* name spaces. The name DNS!! also resolves to another, unique principal in all name spaces. Note that this does not mean that all principals have a single, unique global name. Rather, a principal can have multiple global names that start from different distinguished roots (as in our example).

### 3.3.4 SDSI Groups

SDSI allows its principals to define groups, or sets, of principals. Each group has a name and a set of members. The name is local to some principal, which is the "owner" of the group. Only a group's owner may change its definition. A group can be an explicit list of the group's members (either as a list of principals and/or names of principals), or it can be defined in terms of other groups. Any principal can define his own groups and export them via his servers in much the same way as name bindings. The servers can issue membership certificates based on the groups' definitions.

Groups provide the fundamental mechanism by which SDSI operates. When defining a security policy (for example, specifying who is allowed access to a particular resource), SDSI allows you to define the group of authorized principals, then place the group's name on the resource's access-control list(s). SDSI's nam-

ing system allows a person to easily understand security policies created in this way.

### 3.3.5 SDSI in Action

To better illustrate SDSI's ideas, we now provide a small example of how SDSI would operate in a typical situation. SDSI defines *protocols* in which *messages* are exchanged. Our example, illustrated in Fig. 3.10, shows how the SDSI Membership and Get protocols are used to access an FTP server.

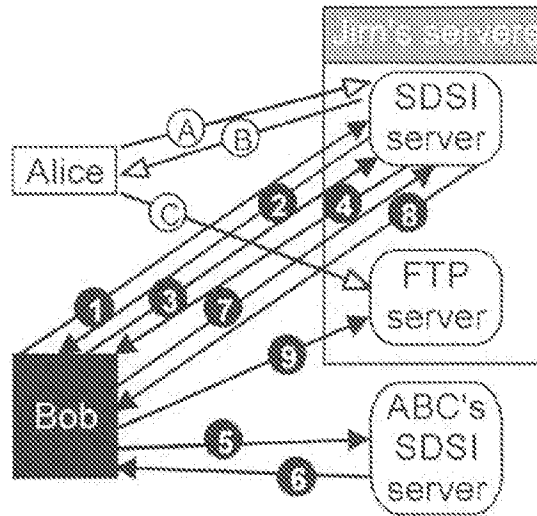


Fig. 3.11 SDSI protocol example

The FTP server is administered by Jim, an employee of ABC Inc. Jim wants to give FTP access to his friends and to other ABC employees. Jim defines a group called ftp-users on his SDSI server. That group contains two entries, the groups named friends and abc's employees, meaning that for a principal to be a member of the ftp-users group it must either be a member of friends or a member of abc's employees (or both). Jim has also defined a group he calls friends on his server, which contains the names alice, stanley and Bob, corresponding to the principals of Jim's friends. Furthermore, Jim has bound the name abc to ABC Inc.'s principal. Finally, ABC Inc. has created a group it calls employees on its SDSI server, which lists all the principals of its employees, including one that they have named BobSmith103456, which is Bob's principal. These group definitions are shown in Fig. 3.11.

We begin our example by illustrating how Jim's friend Alice gains FTP access, then follow with the more complicated example of how Bob gains the same access. The messages sent and received by Alice are depicted in Fig. 3.10 with white-headed arrows, while those involving Bob are shown with black-headed arrows.

To gain access to the FTP server, Alice must show that she is a member of Jim's ftp-users group. She sends a SDSI Membership.Query message (arrow A in Fig. 3.10) to Jim's SDSI server, in which she specifies her principal and the group

name ftp-users. The message is a request for a certificate stating the membership status of the given principal for the given group. That status may be one of true (i.e., the principal is a member), false (is not a member) or fail (may or may not be a member, additional credentials are needed for a full determination).

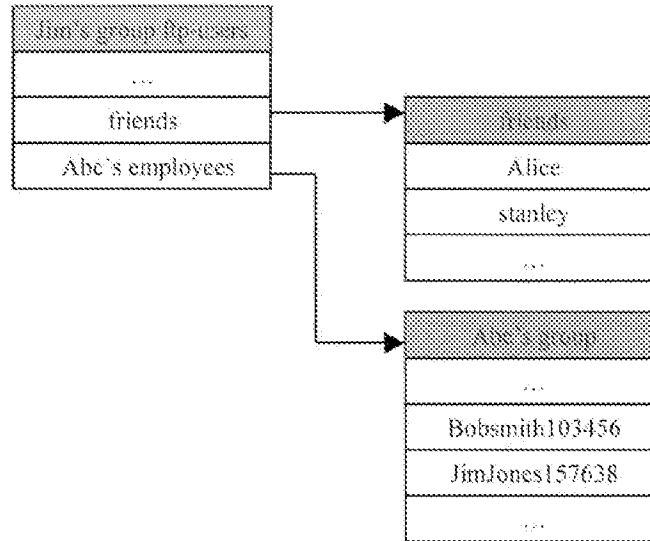


Fig. 3.12 Sample SDSI groups

In Alice's case when Jim's SDSI server performs the membership check it finds that the principal that Jim has named alice matches the principal in the Membership.Query message and is a member of Jim's friends group, which satisfies the membership requirements for the ftp-users group. Jim's SDSI server replies to Alice's query with a true membership certificate for Alice's principal (arrow B). Alice then presents the membership certificate to Jim's FTP server (arrow C) to gain access.

Bob's case is a bit more complicated. Bob is an employee of ABC Inc. but his principal is not a member of Jim's friends group. When Bob sends a Membership.Query to Jim's SDSI server (arrow 1), the reply (arrow 2) is a fail membership certificate along with an indication that if Bob can show membership (or non-membership) in Jim's abc's employees group it would help in determining his membership in the ftp-users group.

Bob needs to find out which principal Jim has named abc, so he sends a SDSI Get protocol Get.Query message to Jim's SDSI server (arrow 3). The Get protocol is used to retrieve certificates from a server. In this case, Bob requests all of Jim's

name-binding certificates that specify the local name abc. Jim's SDSI server replies with a certificate showing that Jim's local name abc corresponds to ABC Inc.'s principal (arrow 4).

Bob now contacts ABC's SDSI server with a Membership.Query message for the employees group (arrow 5). ABC's SDSI server finds that Bob's principal is a member of the group, and returns a true membership certificate (arrow 6). Now Bob can send another ftp-users Membership.Query message (arrow 7) to Jim's SDSI server, this time including the membership certificate he obtained from ABC's SDSI server. Using this new credential, Jim's SDSI server can verify that Bob is a member of the ftp-users group and return a true membership certificate (arrow 8) which Bob can present to the FTP server to gain access (arrow 9).

### 3.3.6 The Simple Public Key Infrastructure

At the beginning of 1996, just before the publication of the SDSI paper, an Internet working group was formed to propose an alternative PKI to the X.509v3-based PKIX. This new group is called the simple public key infrastructure (SPKI) Working Group. So far, the group has only published a requirements statement, [3.59], and a draft certificate format, [3.58].

There are several similarities between the SPKI and SDSI. In particular, one of the SPKI's requirements is to support, where possible, the SDSI local name space mechanism. SDSI is, and the SPKI will be, key-centric (SDSI speaks of principals" while the SPKI uses the term keyholders"), and both provide a mechanism for attaching credentials (the SPKI calls them attributes) to public key values (SDSI through its groups, the SPKI by issuing certificates).

Although the SPKI will use SDSI names, it considers global naming schemes to be irrelevant. To quote the SPKI requirements document: "A user of a certificate needs to know whether a given keyholder has been granted some attribute and that attribute rarely involves a name." The SPKI recognizes the need to uniquely identify keyholders, and considers the public key value itself (or its hash) adequate for that purpose.

The SPKI will be a credential-based system. Its certificates will carry the minimum attributes necessary to get a job done. This is to protect, as much as possible, the privacy of keyholders. Using monolithic certificates that contain many attributes, most of which are irrelevant in a given situation, would reveal more information about the keyholder than he might like. Also, to discourage keyholders from sharing their private key values, the SPKI will allow a certificate holder to delegate the attributes she acquires from the certificate. Finally, SPKI certificates are to have several validation and revocation mechanisms: validity periods, peri-

odic reconfirmation, CRLs, or some user-defined conditions to be tested online or through other certificates.

### 3.4 Summary

This chapter introduces the basic concept of PKI. There are several international PKI standards. Among them, X.509 has been widely used around the world. Many companies have released their PKI products for various applications, especially for e-business. Much recent work has focused on moving away from identity-based PKIs, such as X.509, to a more general system based on attributes or credentials. There are two main proposals for this kind of system: the simple distributed security infrastructure (SDSI), and the simple public key infrastructure (SPKI). These two proposals will play an important role in some special enterprise applications.

### 3.5 References

- [3.1] M. Blaze, J. Feigenbaum, J. Lacy (1996) Decentralized trust management. In: Proceedings of the IEEE Conference on Security and Privacy.
- [3.2] Data Encryption Standard (1993) Federal Information Processing Standards Publication 46-2.
- [3.3] W. Diffie, M. E. Hellman (1976) New directions in cryptography. IEEE Trans Infor Theory 22: 644–654.
- [3.4] C. Liu, P. Albitz (1992) DNS and BIND. O'Reilly, Beijing Cambridge Farnham Koln Tokyo.
- [3.5] T. ElGamal (1985) A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Infor Theory 31: 469–472.
- [3.6] C. M. Ellison (1996) Generalized certificates.
- [3.7] C. H. Fancher (1996) Smart cards. Scientific American 275(2): 40–45.
- [3.8] W. Ford (1995) Advances in public-key certificate standards. ACM SIGSAC Security Audit & Control Review 13(3).
- [3.9] W. Ford (1995) A public key infrastructure for US government unclassified but sensitive applications. Produced by Nortel and BNR for NIST.
- [3.10] W. Ford, M. Baum (1997) Secure electronic commerce: building the infrastructure for digital signatures and encryption. Prentice-Hall, Englewood Cliffs New York.
- [3.11] M. Froomkin: The essential role of trusted third parties in electronic commerce.
- [3.12] Government of Canada (1995) The challenge of the Information Highway: Final Report of the Information Highway Advisory Council.

- [3.13] M. Branchaud (1997) A survey of public-key infrastructures. Master's degree thesis, McGill University.
- [3.14] N. McBurnett: PGP Web of trust statistics.
- [3.15] N. Negroponte (1995) Being digital. Alfred A. Knopf, New York.
- [3.16] Public Key Infrastructure Study Final Report (1994) Produced by the MITRE Corporation for NIST.
- [3.17] W. Polk (ed.) (1996) Federal public key infrastructure (PKI) technical specifications (version 1) Part A: requirements. NIST PKI Technical Working Group.
- [3.18] N. Nazareno (ed.) (1996) Federal public key infrastructure (PKI) technical specifications (version 1) Part B: technical security policy. NIST PKI Technical Working Group.
- [3.19] W. Burr (ed.) (1995) Federal public key infrastructure (PKI) technical specifications (version 1) Part C: concept of operations. NIST PKI Technical Working Group.
- [3.20] Federal public key infrastructure (PKI) technical specifications (version 1) Part D: interoperability profiles (1995) Produced by CygnaCom Solutions, Inc. for the NIST PKI Technical Working Group.
- [3.21] D. Trcek, B. J. Blazic (1995) Certification infrastructure reference procedures. NIST PKI Technical Working Group (W. Burr, ed), NISTIR 5788, NIST.
- [3.22] M. S. Baum (1994) Certification authority liability and policy. NIST-GCR-94-654, NTIS Doc. No. PB94-191-202. National Technical Information Service, Springfield, VA.
- [3.23] B. S. Jr. Kaliski (1993) An overview of the PKCS standards. RSA Laboratories.
- [3.24] RSA Laboratories (1993) PKCS #10: certification request standard.
- [3.25] RSA Laboratories (1993) PKCS #6: extended-certificate syntax standard.
- [3.26] RSA Laboratories (1993) PKCS #9: selected attribute types.
- [3.27] R. Housley, W. Ford, D. Solo: Internet public key infrastructure, Part I: X.509 certificate and CRL profile (draft). IETF X.509 PKI (PKIX) Working Group.
- [3.28] S. Farrell, C. Adams, W. Ford: Internet public key infrastructure, Part III: certificate management protocols (draft). IETF X.509 PKI (PKIX) Working Group.
- [3.29] M. Stahl (1987) Domain administrators guide. RFC1032.
- [3.30] M. Lottor (1987) Domain administrators operations guide. RFC1033.
- [3.31] P. Mockapeteris (1987) Domain names – concepts and facilities. RFC1034.
- [3.32] P. Mockapeteris (1987) Domain names – implementation and specification. RFC1035.
- [3.33] R. Rivest (1992) The MD5 message-digest algorithm. RFC1321.
- [3.34] J. Linn (1993) Privacy enhancement for Internet electronic mail, Part I: message encryption and authentication procedures. RFC1421.
- [3.35] S. Kent (1993) Privacy enhancement for Internet electronic mail, Part II: certificate-based key management. RFC1422.

- [3.36] D. Balenson (1993) Privacy enhancement for Internet electronic mail, Part III: algorithms, modes, and identifiers. RFC1423.
- [3.37] B. Kaliski (1993): Privacy enhancement for Internet electronic mail, Part IV: key certification and related services. RFC1424.
- [3.38] J. Kohl, B. C. Neuman (1993) The Kerberos network authentication service (version 5). RFC1510.
- [3.39] C. Malamud, M. Rose (1993) Principles of operation for the TPC.INT subdomain: general principles and policy. RFC1530.
- [3.40] R. Atkinson (1995) Security architecture for the Internet protocol. RFC1825.
- [3.41] J. Galvin, S. Murphy, S. Crocker, N. Freed (1995) Security multipart for MIME: multipart/signed and multipart/encrypted. RFC1847.
- [3.42] D. Eastlake, C. Kaufman (1997) Domain name system security extensions. RFC2065.
- [3.43] R. Housley, W. Ford, W. Polk, D. Solo (1999) Internet X.509 public key infrastructure certificate and CRL profile. RFC2459.
- [3.44] C. Adams, S. Farrell (1999) Internet X.509 public key infrastructure certificate management protocols. RFC2510.
- [3.45] M. Myers, C. Adams, D. Solo, D. Kemp (1999) Internet X.509 certificate request message format. RFC2511.
- [3.46] S. Chokhani, W. Ford (1999) Internet X.509 public key infrastructure certificate policy and certification practices framework. RFC2527.
- [3.47] R. Housley, W. Polk (1999) Internet X.509 public key infrastructure representation of key exchange algorithm (KEA) keys in Internet X.509 public key infrastructure certificates. RFC2528.
- [3.48] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams (1999) X.509 Internet public key infrastructure online certificate status protocol – OCSP. RFC2560.
- [3.49] R. Housley, P. Hoffman (1999) Internet X.509 public key infrastructure operational protocols: FTP and HTTP. RFC2585.
- [3.50] S. Boeyen, T. Howes, P. Richard (1999) Internet X.509 public key infrastructure LDAPv2 schema. RFC2587.
- [3.51] R. Rivest, A. Shamir, L. Adleman (1978) A method for obtaining digital signatures and public key cryptosystems. Commun ACM 21: 120-126.
- [3.52] M. Saeki (1996) Elliptic curve cryptosystems. M.Sc. thesis, McGill University.
- [3.53] B. Schneier (1996) Applied cryptography (2nd ed). Wiley, New York.
- [3.54] R. Rivest, B. Lampson (1996) SDSI – A simple distributed security infrastructure.
- [3.55] MasterCard and Visa (1996) Secure electronic transaction (SET) specifications.
- [3.56] Secure Hash Standard (1995) Federal information processing standards publication 180-1.
- [3.57] D. R. Stinson (1995) Cryptography: theory and practice. CRC Press, Boca Raton New York.

- [3.58] C. M. Ellison, B. Frantz, B. M. Thomas (1996) Simple Public Key Certificate.
- [3.59] C. M. Ellison (1997) SPKI requirements.
- [3.60] D. Trcek, B. J. Blazic, N. Pavesic (1996) Security policy space definition and structuring. *Computer Standards & Interfaces* 18(2): 191–195.
- [3.61] D. Trcek, T. Klobucar, B. J. Blazic, F. Bracun (1994) CA-browsing system – A supporting application for global security services. In: ISOC Symposium on Network and Distributed System Security, pp. 123–128.
- [3.62] ITU/ISO (1988) Recommendation X.208. Specification of abstract syntax notation one (ASN.1).
- [3.63] ITU/ISO (1998) Recommendation X.209. Specification of basic encoding rules for abstract syntax notation one (ASN.1).
- [3.64] ITU/ISO (1993) Recommendation X.500. Information technology – open systems interconnection – the directory: overview of concepts, models, and services.
- [3.65] ITU/ISO (1993) Recommendation X.509. Information technology – open systems interconnection – the directory: authentication framework.
- [3.66] ITU/ISO (1996) Final text of draft amendments to X.500/9594 for certificate extensions.
- [3.67] P. Zimmermann: PGP user’s guide vol. 1 and 2.



## 4 Biometrics for Security in E-Commerce

David Zhang<sup>1</sup> and Li Yu<sup>2</sup>

<sup>1</sup> Department of Computing  
Hong Kong Polytechnic University, Hong Kong

<sup>2</sup> Department of Computer Science and Technology  
Harbin Institute of Technology, China

### 4.1 An Overview of Biometrics

The advance of technology is always inspired by the practical applications, and the emergence of automatic biometrics technology is rooted in the requirement for real-world security applications. Whether this new technology can last for a long time will be decided by how well it can solve security problems. Although biometric technology is at the development stage, it has been implemented in various applications and some of them work well. Along with the widespread application of biometrics technology, more funds and more attention are being given to this ascending technology [4.1-4.4, 4.20-4.22, 4.24, 4.32, 4.34].

Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics [4.19]. Today a variety of biometric technologies are used, each with its own strengths to make it more appropriate than others for certain types of applications. Fig. 4.1 shows the major biometric technologies:

- Finger-scan
- Hand-scan, aka, hand geometry
- Retina-scan
- Iris-scan
- Facial-scan, aka, facial geometry
- Signature-scan, aka, dynamic signature verification
- Voice-scan, aka, voice or speaker verification

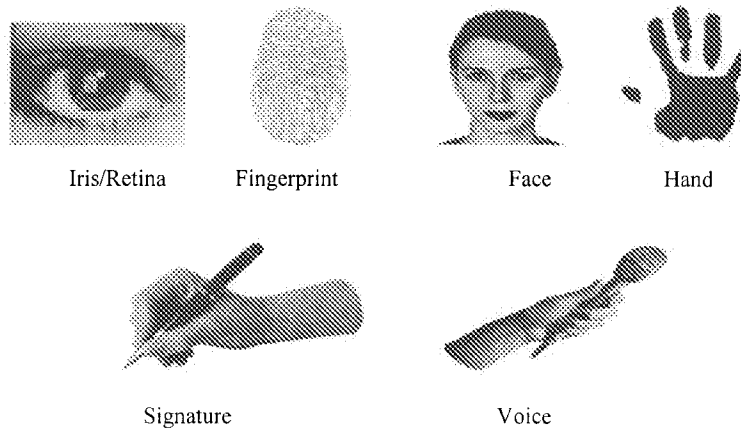


Fig. 4.1 Biometrics technologies

Biometric is the most secure and convenient authentication tool. It cannot be borrowed, stolen, or forgotten, and forging one is practically impossible. Common physical biometrics includes fingerprints, hand or palm geometry, retina, iris, and facial characteristics. Behavioral characteristics include a person's signature, voice (which also has a physical component), keystroke pattern, and gait. Technologies for signature and voice are the most developed for the behavioral biometrics [4.30-4.33, 4.35].

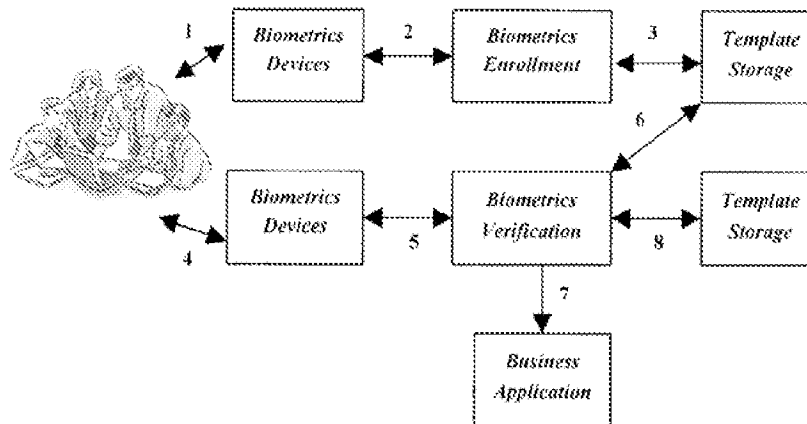


Fig. 4.2 How a biometric system works

In Fig. 4.2 the process involved in using a biometric system is described. The text descriptions of these processes are as follows:

- (1) Capture the chosen biometric data.
- (2) Process the biometric data, extract it and enroll it to form a biometric template.
- (3) Store the template in a local repository, a central repository, or a portable token such as a smart card.
- (4) Live-scan the chosen biometric.
- (5) Process the biometric data and extract features to form a biometric template.
- (6) Match the new template against stored templates.
- (7) Calculate a matching score for the business application.
- (8) Record a secure audit trail with respect to system use.

#### 4.1.1 Finger-Scan Technology

Finger-scan biometrics is based on the distinctive characteristics of the human fingerprint. A fingerprint image is read from a capture device, features are extracted from the image, and a template is created. If appropriate precautions are followed, the result is a very accurate means of authentication [4.2-4.4, 4.6-4.8, 4.23, 4.27].

Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation-based [4.25]. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties for this approach when the fingerprint is of such low quality such that accurate extraction of minutiae points is difficult. Also, this method does not take into account the global pattern of ridges and furrows. In contrast, the correlation-based method is able to overcome the problems of the minutiae-based approach. However, correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation.

The most widely used methods of controlling access to computers and data are passwords and PINs. While passwords and PINs are easy to use, they provide weak proof of identity. They are rarely changed, frequently shared, often used in plain sight, and easily defeated using widely available hacker programs. Implementing fingerprint authentication and replacing passwords and PINs makes access to corporate information more efficient and secure. Fingerprint verification may be a good choice for in-house systems that operate in a controlled environment where you can give users adequate explanation and training. A fingerprint authentication solution can provide secure online banking transactions, secure customer financial information, new online services, and non-repudiation. The benefits include fraud protection, customer confidence and retention, time/cost efficiencies, and the ability to extend services to non-local customers.

#### 4.1.2 Hand-Scan Technology

This approach uses the geometric shape of the hand for authentication. Authentication of identity using hand geometry is challenging work, as hand features are not very descriptive. The problem can be tackled by combining various individual features to attain robust verification [4.2-4.4].

Hand-scan is occasionally misunderstood as “palm reading,” as the placement of the hand palm-down on the reader can be confusing to those unfamiliar with the technology.

Hand-scan is a relatively accurate technology, but does not draw on as rich a data set as finger-, face-, or iris-scans. A decent measure of the distinctiveness of a biometric technology is its ability to perform one-to-many searches, that is, the ability to identify a user without the user first claiming an identity. Hand-scan does not perform one-to-many identification very well, as similarities between hands are not uncommon. It has an advantage in failure-to-enroll (FTE) rates, which measures the likelihood that a user is incapable of enrolling in the system. In contrast, finger-scan is prone to FTEs in the case of poor-quality fingerprints, and facial-scan requires consistent lighting to properly enroll a user. Since nearly all users will have the dexterity to use hand-scan technology, only a few employees and visitors will need to be processed outside the biometric.

Organizations use hand-geometry readers in various scenarios, including time and attendance recording, where they have proved extremely popular. Hand-scan technology offers the following benefits:

- (1) Cards and associated administration costs can be eliminated.
- (2) “Buddy-punching” is impossible; this is particularly rated by leading time and attendance software systems.
- (3) True-time clock functionality including department transfers, supervisor override, and time restrictions.

Various applications, such as credit card and ATM transactions, check cashing, and even picking up a child from daycare, benefit from this technology.

The benefits of hand-geometry scanning in personal identification are:

- (1) High user acceptance, non-intrusive technology.
- (2) Fast and easy enrollment use.
- (3) Low false reject rate equates to a positive user experience.

Ease of integration into other systems and processes, coupled with ease of use, makes hand-geometry scanning an obvious first step for many biometric projects.

#### 4.1.3 Retina-Scan Technology

Along with iris recognition technology, retina scan is perhaps the most accurate and reliable biometric technology. However, it is difficult to use and is perceived as being moderately to highly intrusive. In films, portrayals of retina-scan devices reading at an arm's length, with a non-stationary subject, are false. Retina-scan biometrics requires a cooperative, well-trained, patient audience, or else performance will fall dramatically [4.2, 4.4-4.5].

Even when those unfamiliar with the rudimentary anatomy of the eye are reminded that all vision is based upon light passing through the pupil to the retina, there is still notable resistance to retina-scan technology. This is perhaps due to an unusually high degree of sensitivity on issues of the eye; iris-scan biometrics, where the patterns of the iris are read, which requires less effort on the part of the user, is also frequently met with similar expressions of hesitation.

Retina-scan devices read through the pupil; this requires the user to situate their eye within 1/2 inch of the capture device, and to hold still while the reader ascertains the patterns. The user looks at a rotating green light as the patterns of the retina are measured at over 400 points. By comparison, a fingerprint may only provide 30-40 distinctive points (minutiae) to be used in the enrollment, template creation, and verification process. Retina-scanning has a very high level of accuracy compared to most other biometrics.

Retina-scanning can be quite accurate but requires the user to look into a receptacle and focus on a given point. This is not particularly convenient if you wear glasses or are concerned about having close contact with the reading device. For these reasons, retina-scanning is not warmly accepted by all users, even though the technology itself works well.

#### 4.1.4 Iris-Scan Technology

Iris recognition uses the unique features of the human iris to provide an unmatched identification technology. So accurate are the algorithms used in iris recognition that the entire planet could be enrolled in an iris database with only a small chance of false acceptance or false rejection [4.2, 4.4-4.5].

Iris identification technology is a tremendously accurate biometric. Only retina-scan can offer nearly the security that iris-scan offers, and the interface for retina-scan is thought by many to be more challenging and intrusive. More common biometrics provide reasonably accurate results in verification schematics, whereby the biometric verifies a claimed identity, but they cannot be used in large-scale identification implementations like iris recognition.

An iris-based biometric, on the other hand, involves analyzing features found in the colored ring of tissue that surrounds the pupil. Iris-scan, undoubtedly the less intrusive of the eye-related biometrics, uses a fairly conventional camera element and requires no close contact between the user and the reader. In addition, it has the potential for a higher than average template-matching performance. Iris biometrics work with glasses in place and it is one of the few technologies that can work well in identification mode. Ease of use and system integration have not traditionally been strong points with iris-scanning devices, but you can expect improvements in these areas as new products emerge.

In some banks, new ATMs with iris-recognition technology have been used to control access to bank accounts. After enrolling once (a “30 second” process), the customer needs only to approach the ATM, follow the instruction to look at the camera, and be recognized within 2-4 seconds [4.44].

Again, the benefits of such a system are clear, that is, the customer who chooses to use an ATM with iris recognition will have a quicker, more secure transaction. Although one may question whether the risk of fraud at ATM's is very large, this type of integration makes long-term sense. First, ATMs are large, omnipresent, secured devices which, the public knows, visually record every transaction. It is a small cognitive leap to envision them moving from their current configuration to being biometrically enabled. Second, iris technology is being put before the public in a non-coercive, unobtrusive, fairly low-risk setting. As the accuracy and reliability of the technology are proven through time, the public should be accepting of less traditional implementations. Like the vast majority of biometric companies, iris recognition vendors are very eager to participate in securing Internet commerce. The potential market for the vendors whose technology is most widely embraced is unimaginably large.

#### **4.1.5 Facial-Scan Technology**

Similar to finger-scan and voice-scan biometrics, there are various methods by which facial-scan technology recognizes people. All share certain commonalities, such as emphasizing those sections of the face that are less susceptible to alteration, including the upper outlines of the eye sockets, the areas surrounding the cheekbones, and the sides of the mouth. Most technologies are resistant to moderate changes in hairstyle, as they do not utilize areas of the face located near the hairline. All of the primary technologies are designed to be robust enough to conduct one-to-many searches, that is, to locate a single face out of a database of thousands, and even hundreds of thousands, of faces [4.2, 4.4-4.5, 4.27].

Facial-scans can be used to control entry to buildings or computer networks by comparing the image of a person seeking access against the scan taken of that person at an earlier date, that is, a one-to-one check [4.47].

Facial-recognition solutions employ the same four-step process that all biometric technologies do, namely, sample capture, feature extraction, template comparison, and matching. The sample capture takes place in the enrollment process, during which the system takes multiple pictures of the face, usually from slightly different angles, to increase the system's ability to recognize the face. After enrollment, certain facial features are extracted and used to create a template. The specific features extracted vary depending on the type of facial-recognition technology used. No images of faces are stored. Instead, the templates consist of numeric codes that are usually encrypted. Many templates can be stored on one system because each is less than 1K in size, compared to between 150K and 300K for a facial image. When someone logs in using a facial-scan system, the template created upon attempted login is compared to a stored template for that person (one-to-one matching) or to a database of stored templates (one-to-many matching).

Face recognition involves the analysis of facial characteristics. This technique has attracted considerable interest, although many people do not completely understand its capabilities. Some vendors have made extravagant claims, which are very difficult, if not impossible, to substantiate in practice for facial-recognition devices. Because facial-scanning needs an extra peripheral not customarily included with basic PCs, it is more of a niche market for network authentication. However, the casino industry has capitalized on this technology to create a facial database of scam artists for quick detection by security personnel.

#### **4.1.6 Handwriting and Signature Verification**

Signature verification involves analysis of the way a user signs their name. Signing features, such as speed, velocity, and pressure, are as important as the finished signature's static shape. Signature verification enjoys a synergy with existing processes that other biometrics do not. People are used to signatures as a means of transaction-related identity verification, and most would see nothing unusual in extending this to encompass biometrics. Signature-verification devices are reasonably accurate in operation and obviously lend themselves to applications where a signature is an accepted identifier.

Electronic-signature verification is also gaining ground for retail and e-commerce applications. The implementation includes installation of electronic-signature software and the solution utilizes electronic signatures to automate processing of some lease-end documents. The solution is part of a transition from paper lease-end documents to electronic documents, which will reduce operation

costs and provide an easy-to-use, legally binding electronic signature. E-Pad [4.45] captures a handwritten signature and converts it to a biometric e-signature, offering enhanced workflow and faster processing times. Electronic signatures may be bound into Microsoft Word and Outlook documents, Adobe Acrobat files, and many other forms and transactions. They also feature a handwriting profile that can be used to authenticate the identity of the signer. Surprisingly, relatively few significant signature applications have emerged compared with other biometrics methodologies. But if your application fits, it is a technology worth considering [4.2, 4.4-4.5].

#### **4.1.7 Voice-Scan Technology**

Of all the above-mentioned human traits used in biometrics, the one that humans learn to recognize first is the voice characteristic. Infants can identify the voice of their mothers and telephone users can identify a caller on a noisy telephone line. Furthermore, the bandwidth associated with speech is much smaller than the other image-based human traits. This implies quicker processing and smaller storage space [4.2, 4.4-4.5, 4.26, 4.29].

A speaker-recognition system can be divided into two categories, namely, text-dependent and text-independent systems. In text-dependent systems, the user is expected to use the same text (keyword or sentence) during training and recognition sessions. A text-independent system does not use the training text during recognition session. Both systems perform the following tasks: feature extraction, similarity analysis, and selection. Texture extraction uses the spectral envelope to adjust a set of coefficients in a predictive system. One voice sample can then be compared for similarity with another sample by computing the regression between the coefficients. This is a similarity analysis. A number of normalization techniques have been developed to account for variation of the speech signals.

A voice security system is responsible for an innovative method of security that dramatically reduces fraud and can prevent one's property from being use, if stolen or obtained fraudulently. This new breakthrough allows speaker-verification to be burned onto an existing microprocessor within a device. Examples of use of this technology are cell phones (to eliminate cell phone fraud), ATMs (to eliminate PIN fraud), and automobiles (to dramatically reduce theft and carjacking). This method is the only standalone technology that does not require management of a large user database, thus protecting the privacy of the user's biometric data. The software, algorithms and templates can be stored on the microprocessor that a device already employs to operate the functions of the electronic hardware inside [4.42].



Voice authentication is not based on voice recognition but on voice-to-print authentication, where complex technology transforms voice into text. Voice biometrics has the most potential for growth, because it does not require new hardware, that is, most PCs nowadays already come with a microphone. However, poor voice quality and ambient noise can affect verification. In addition, the enrollment procedure has often been more complicated than with other biometrics, leading to the perception that voice verification is not user friendly. Therefore, voice authentication software needs improvement. One day, voice may be integrated with finger-scan technology. Because many people see finger-scanning as a higher form of authentication, voice biometrics will most likely be relegated to replace or enhance PINs, passwords, or account names.

## 4.2 Potential Application Areas

Biometrics applications are not limited to the areas mentioned in the last section. In fact, as long as a system needs to recognize people, it can incorporate biometrics. In the law enforcement community, matching finger images or part of palm images is the most common method to process criminal suspects and bring guilty criminals to justice. Also we have seen many times in movies the police ask the witness to describe the criminal's physical features such as hair color, the length, width, and shape of the face, etc.; and they then reconstruct a picture of the criminal. In some movies, we see the criminal call the victim over the phone and the police can record the voice of the criminal and search for the criminal according to the voice. All these scenes are examples of finding people using their unique physical features (finger, palm, face, etc.) or behavioral trait (voice), and automatic biometrics can help in all these examples. It is not difficult to understand that the law enforcement community is the largest biometrics user group. Police forces throughout the world are using the Automatic Fingerprint Identification System to assist in crime detection. There are many biometrics vendors earning significant revenues in this area [4.9, 4.11-4.12, 4.14-4.15].

Businessmen always play an important role in spreading a new technology. As automatic biometrics technologies become more and more mature in the law enforcement area, they are also introduced in civilian applications by biometrics product vendors. Usually most civilian biometrics applications are some kind of access control. We may simply classify all the civilian biometrics applications as either physical access control or data access control. Physical access control ensures only authorized individuals can physically access secure areas while data access control secures access to sensitive data. Securing benefit systems against fraud, preventing illegal immigrants from entering a country, or prisoners from leaving a prison all belong to physical access control, while Internet banking, telephone banking, ATM, and Web Store belong to data access control. Automatic biometrics is a rapidly expanding market. Fraud is an ever-increasing problem and

security is becoming a necessity in many walks of life. Civilian access control, therefore, will not be restricted to the application areas mentioned below and will branch out to other market opportunities as soon as a need is identified.

#### **4.2.1 Benefit Systems**

When applying biometrics in benefit systems, it plays a different role from that in banking or in physical access control. In banking or physical access control or other methods of access control, all unique physical features or behavioral traits are registered in a system before the system is used. When somebody needs to access the system, their unique feature is captured at that point and the system checks the newly captured feature against the template in the database to decide whether it is from the same person. This will prevent unauthorized people from accessing the system. In benefit systems, however, people do not need to register their features first. Only when they need to get the benefit is their unique feature extracted and stored in the system. The system checks whether this person has already registered and received the benefit before, by checking the database templates. Biometrics is well placed to capitalize on this phenomenal market opportunity, and vendors are building on the strong relationship currently enjoyed with the benefits community.

#### **4.2.2 E-Commerce Applications**

E-commerce developers are exploring the use of biometrics and smart cards to more accurately verify a trading party's identity. For example, many banks are interested in this combination to better authenticate customers and ensure non-repudiation of online banking, trading, and purchasing transactions [4.5, 4.9, 4.13].

Banks may embrace biometrics technologies from various aspects. Automated teller machines (ATMs) and transactions at the point of sale, telephone banking, Internet banking, and many other banking applications are vulnerable to fraud and can be secured by biometrics. Fig. 4.3 shows various biometrics and banking services and where they can be applied.

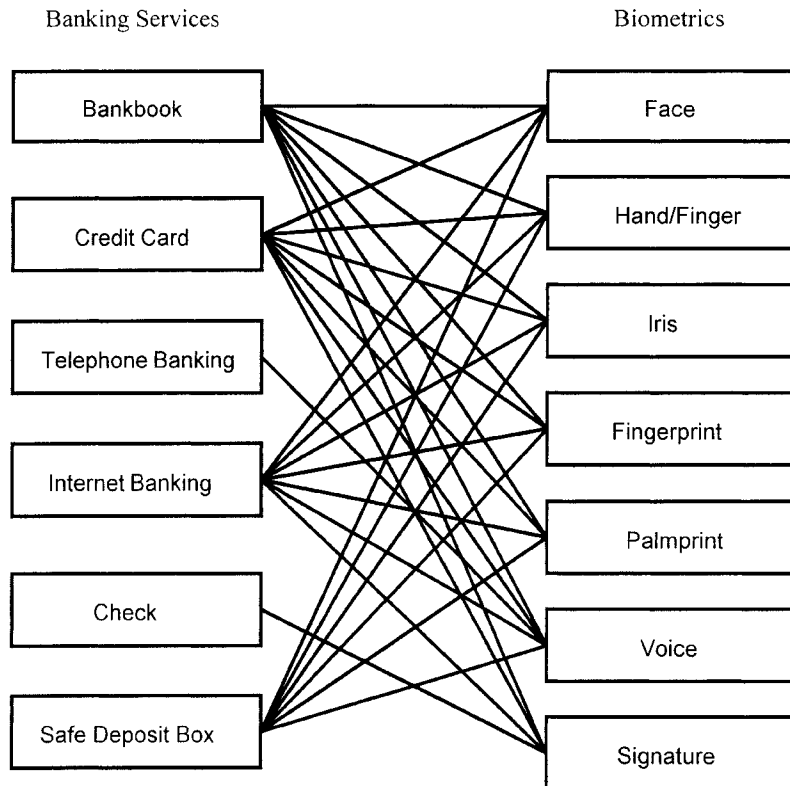


Fig. 4.3 Biometrics applications in banking

Point-of-sale (POS) system vendors are working on the cardholder verification method, which would enlist smart cards and biometrics to replace signature verification. MasterCard estimates that adding smart-card-based biometric authentication to a POS credit card payment will decrease fraud by 80%.

Merchants use biometrics to obtain secure services over the telephone through voice authentication. Voice authentication systems developed by Nuance Communications are currently deployed nationwide, by both the Home Shopping Network and Charles Schwab. The latter's marketing catch phrase is: "No PIN to remember, no PIN to forget."

#### **4.2.3 Computer Systems**

Currently, computer systems use passwords as their secure guards. On one hand, remembering tens of passwords and changing passwords very often becomes a headache for almost everyone who uses a computer; on the other hand, a password itself does not have direct connection to the end-user. If somebody gets the password, they will be considered as a legal user by the computer system even though he is a criminal and meanwhile, if a legal user forgets their password, they will be refused access to their own computer. Biometrics technology binds the authority directly to the end-user and removes the need for various passwords. Voice and fingerprint recognition are now the most promising techniques in this area.

#### **4.2.4 Immigration**

Terrorism, drug-running, illegal immigration, and an increasing throughput of legitimate travelers are putting a strain on immigration authorities throughout the world. It is essential that these authorities can quickly and automatically process law-abiding travelers and identify the lawbreakers. Biometrics is being employed in a number of diverse applications to make this possible. The US Immigration and Naturalization Service is a major user and evaluator of a number of biometrics. Systems are currently in place throughout the US to automate the flow of legitimate travelers and deter illegal immigrants. Elsewhere biometrics is capturing the imagination of countries such as Australia, Bermuda, Germany, Malaysia, and Taiwan.

#### **4.2.5 National Identity**

Biometrics is beginning to assist governments as they record population growth, identify citizens, and prevent fraud occurring during local and national elections. Often this involves storing a biometrics template on a card that in turn acts as a national identity document. Finger scanning is particularly strong in this area and schemes are already under way in Jamaica, Lebanon, The Philippines, and South Africa.

#### **4.2.6 Telephone Systems**

Global communication has truly opened up over the past decade, while telephone companies are under attack from fraud. Once again, biometrics is being called upon to defend this onslaught. Speaker ID is a technique for recognizing people by

their voices. It is obviously well suited to the telephone environment and is catching these new markets quickly.

#### **4.2.7 Monitoring Time and Attendance**

Currently, some factories and companies use cards to monitor the movement of their employees. When they come to work, they need to punch a hole on their cards and another hole when they leave. Such things can be assisted by biometrics. With a biometrics system, employees may press their fingers on a small platform when they come or leave. This may prevent some forms of cheating. But using such a system to monitor employees' movement is still in question because some people think it may violate an employee's privacy.

#### **4.2.8 Covert Surveillance**

One of the more challenging research areas involves using biometrics for covert surveillance. Using facial and body recognition technologies, researchers hope to use biometrics to automatically identify known suspects entering buildings or traversing crowded security areas such as airports. The use of biometrics for covert identification as opposed to authentication must overcome technical challenges such as simultaneously identifying multiple subjects in a crowd and working with uncooperative subjects. In these situations, devices cannot count on consistency in pose, viewing angle, or distance from the detector.

### **4.3 Multiple Authentication Technologies**

From an application standpoint, widespread deployment of a user authentication solution requires support for an enterprise's heterogeneous environment. Support for legacy applications, client-server applications, and Web-based applications is extremely important. However, the complexity of this process is exacerbated by the number of application-specific identities one has to manage. This is compounded by the fact that individual authentication devices or methods may be required to maintain additional identities [4.2, 4.5, 4.11, 4.16].

When it comes to selecting and deploying specific verification methods for enterprise-wide use, one size does not fit all. Any solution should enable the selection of different methods, depending on the users, and be flexible enough to enable dynamic, multifactor authentication, allowing you to dial up the appropriate level of security without sacrificing convenience.

The distributed environment of an enterprise – organizationally, geographically, and technologically – means that employees access information from various access channels. For example, an employee who may access data from their desktop one day may use their laptop remotely the next day. The increasing use of PDA and other wireless devices makes it obvious that users must be authenticated regardless of the channel of access in the digital environment.

Finally, user authentication as a security infrastructure cannot be considered in isolation, often it is through a multifaceted security approach in which combinations of security solutions are deployed. An authentication solution should seamlessly extend the organization’s existing security infrastructure.

Consolidating and streamlining user authentication enables the creation of an “Authentication Hub,” as shown in Fig. 4.4, providing a single point of control to deploy and manage a combination of authentication methods such as passwords, smart cards, tokens, and biometrics (fingerprint, voice, face, iris, and signature recognition).

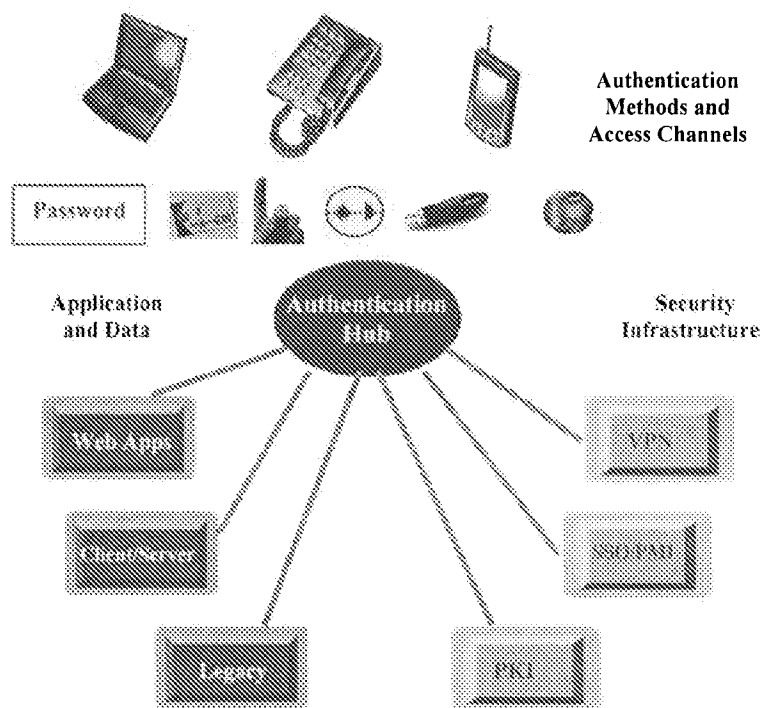


Fig. 4.4 Unified authentication management

An infrastructure that provides unified authentication management allows organizations to manage user authentication through context-based security policies and integrate authentication with existing security solutions such as virtual private networks (VPNs), access management, and public-key infrastructure (PKI). It mitigates interoperability problems between multiple applications, authentication methods, access channels, and platforms, thus driving cost savings, convenience, and security.

When implemented as a strategic component of the security infrastructure within the enterprise, the unified authentication management solution:

- Implements centralized authentication policies for a large number of users.
- Integrates the administration of many forms of authentication.
- Tailors authentication methods to specific information assets, sizes of transactions, roles of individuals and groups, and access channels and entry points.
- Provides a single point for managing user authentication for heterogeneous applications – legacy, client-server, and Web-based.
- Enables convenient but secure access to applications and data in a heterogeneous environment, allowing you to dial up the appropriate level of security without sacrificing user convenience.
- Streamlines the administration tasks necessary to enable convenient and cost effective implementation of strong authentication security policies such as enrollment, verification, policies, and unenrollment of users when multiple authentication methods (smart cards, tokens, fingerprint devices) are deployed.
- Extends existing security infrastructures – VPNs, privilege management (or SSO: single sign-on), policy making and implementation (PMI), and PKI – and seamlessly supports the adoption and migration to advanced authentication methods.

A major problem with biometrics is how and where to store the user's template. Because the template represents the user's personal character, its storage introduces privacy concerns. Furthermore, storing the template in a centralized database leaves that template subject to attack and compromise. On the other hand, storing the template on a smart card enhances individual privacy and increases protection from attack, because individual users control their own templates.

Vendors can enhance security by placing more biometric functions directly on the smart card. Some vendors have built a fingerprint sensor directly into the smart card reader, which in turn passes the biometric to the smart card for verification. At least one vendor, Biometric Associates, has designed a smart card that contains a fingerprint sensor directly on the card. This is a stronger secure architecture because cardholders must authenticate themselves directly to the card.

PKI uses public- and private-key cryptography for user identification and authentication. There are some advantages over biometrics: PKI is mathematically more secure, and it can be used across the Internet. The main drawback of PKI is the management of the user's private key. To be secure, the private key must be protected from compromise; to be useful, the private key must be portable. The solution to these problems is to store the private key on a smart card and protect it with a biometric.

In the Smart Access common government ID card program, the US General Services Administration is exploring this union of biometrics, smart cards, and PKI technology. The government of Finland is also considering using these technologies in the Finnish National Electronic ID card.

## **4.4 How to Select a Biometrics System**

### **4.4.1 Difficulty in Selecting a Biometrics System**

The performance of a biometrics system is greatly impacted by many factors, such as humidity, light, noise, and the end user's attitude to and familiarity with the system. Therefore, for accuracy, testing should be performed in real working circumstances. High levels of accuracy in one application do not qualify a system for an entirely different application. The quoted performance figures of a biometric system only can be applied to the specific application for which they are quoted. Each application is widely different in terms of system workload and throughput, environmental factors, and other variables [4.2, 4.5, 4.17-4.18, 4.28, 4.33, 4.36].

For example, the same fingerprint-verification system may have very high accuracy in a university restaurant while it may work badly in a village where most people have their fingerprints worn heavily.

This is not to say that the performance rulers, the fault accept rate (FAR) and the fault reject rate (FRR) are meaningless, just that the two rates may vary in diverse environments. The FAR and FRR provided by the developer can be used as a guide to understand a system's general ability.

In one sentence, a biometrics system's performance is application sensitive, and making a biometrics system adaptive to a particular application needs significant consideration.



#### **4.4.2 Various Factors: Whether a Biometrics System Is Needed**

Before applying biometrics, we must make clear what the business driver is. What is the main goal of the whole project? What are the constraints of the project, like deadlines, budgets, etc.? What security level is needed? What is the current system? What is the weakness of the current system? Is it necessary to apply biometrics? Can biometrics solve the existing problems? Are there any other choices for securing the system? Will biometrics cause any trouble for the system? Can biometrics integrate well with the current system? Will users of the system accept this new work style? Simply put, making sure biometrics is needed is the first step when applying this new technology.

#### **4.4.3 Comparison of Different Biometrics Techniques**

Tables 4.1 and 4.2 are two tables of comparison for existing biometrics systems. Factors considered in biometrics system evaluation are discussed below.

##### **Vulnerability to Fraud**

Biometrics systems aim at providing high-level security, so whether a biometrics trait is hard to mimic is an essential consideration in the construction of such applications. Extreme measures, such as gouging out eyes or truncating fingers to defraud a biometrics system, have appeared in some movies.

##### **Ease of Use**

One springboard for biometrics system popularity is to allow the public to get rid of the bother of remembering tens of passwords and keeping strings of keys. Such systems could be really user friendly, preventing headaches greater than a lost room key. Some biometric devices are not user friendly. For example, users without proper training may experience difficulty aligning their head with a device for enrolling and matching facial templates, while face, fingerprint, voice, and palm technologies are easy to use.

##### **Intrusive for Human Beings**

Certain biometrics systems are seen to be more intrusive than others. For example, retina capture involves exposing eyes to a bright beam, while voice-scan seems non-intrusive. However, sometimes, a higher accuracy may be gained using a more intrusive approach. Places where high levels of security are needed have to

choose such intrusive methods. For example, workers at a nuclear power plant would probably acknowledge the need for a degree of intrusiveness, as security is a very important issue in that environment.

### **Applicability**

Physical characteristics vary and some individuals will not be able to use a biometrics system. No single biometrics system can capture and match biometrics data for the global population in all circumstances. Human beings are as diverse and unpredictable as environments. Some individuals have damaged fingers, limbs, voice boxes, or eyes. This may make verification and identification with a single biometrics system impossible; but it may be possible to use a multiple-biometrics system. Also, this does not mean that a single biometrics system is unable to perform a task in an application where a minority of people cannot have a biometrics sample captured. It is simply that the minority cannot use the system automatically and must be dealt with in an appropriate manner.

### **Speed of Verification**

Response time is a key issue for any computer system and for biometrics systems.

### **Size of Storage for One Biometrics Template**

For an identification system, this factor directly affects the overall database size and searching speed. For a verification system, where the registered template is stored in some special media such as barcodes, magnetic cards, or smart cards, this factor could determine the cost of a card.

### **Long-Term Stability**

The biometrics feature chosen to identify a person in a system should be stable for at least as long as the system is to be used, so that the system can work correctly during its lifetime.

### **Maturity of Technology**

Some biometrics features, such as fingerprints and signatures, have been used for a long time and their accuracies have been proven widely. Meanwhile, other biometric systems, such as face-scanning and voice-scanning, are newcomers to this area and need to be proven in real-time applications.

From Tables 4.1 and 4.2, retina-scan appears to have the highest crossover accuracy. Even though iris-scan has a high cross over accuracy, its user acceptability is low. Fingerprints and hand geometries are equally “unique.”

Signature dynamics and voice dynamics have the lowest accuracy rates. In addition, these two techniques rely on behavioral measurements as opposed to physical measurements. In general, behavioral biometrics is less reliable than physical biometrics.

Retina-scan has a high accuracy but also has a high data-collection-error rate and a low user-acceptability. For this reason, retina-scan broadly exists only in science fiction movies and not in real-life applications!

The fingerprint biometric has a low data-collection-error rate and a high user-acceptability. Further, fingerprint technology has been heavily invested in, and applied to both the identification and the authentication problem. Finally, fingerprint biometrics has the highest acceptance in the identification community and virtually every large biometrics system in operation today uses fingerprint biometrics. Notwithstanding its association with “criminal” applications, fingerprint biometrics is generally accepted by clients.

Table 4.1 Comparison of various biometrics techniques

<i>Technical factor</i>	<i>Hand geometry</i>	<i>Retina</i>	<i>Fingerprint</i>
False rejection rate	0.2 percent, one try	12.4 percent (one try), 0.4 percent (three tries)	1% - 5%, three tries
False acceptance rate	0.2 percent, one try	0 no false acceptances	0.01 - 0.0001 percent (three tries)
Vulnerability to fraud	Almost impossible to secretly obtain hand-geometry data. However, when the person cooperates, this seems not at all impossible	No counterfeits seem possible. False eyes, contact lenses, or eye transplants cannot breach the security of this device	Dummy fingers and dead fingers will be detected when high-security platen is installed
Ease of use	The first time one needs to get used to it. After some experience it is not difficult	Difficult to use. Socially difficult to accept because people do not like to have their eyes scanned	Easy to use, but it is associated with criminal investigations
Universality	Not suitable for people who have rheumatic hands or related physical impairments	Suitable for everyone with eyes	Not for people with damaged fingerprints due to daily handling of rough material
Speed of identification	Less than 3 seconds	1.5 seconds	Average verification time 2 seconds. Maximum is 20 seconds
Size for storage of template	Only 9 bytes	40 bytes	1203 bytes. After compression it is smaller than 800 bytes
Long-term stability	Sizes of hands will change for children and can change when someone gains or loses a lot of weight	The retinal vascular pattern is very stable. Only a few diseases or injuries will change this pattern	Sizes of fingerprints change for children. Apart from that they always remain the same
Maturity of technology	Worldwide used in many systems	Used in a fair number of systems	Worldwide used in many systems

Table 4.2 Comparison of various biometrics techniques

<i>Technical factor</i>	<i>Iris</i>	<i>Retina</i>	<i>Face</i>	<i>Finger-scanning</i>	<i>Voice</i>	<i>Hand geometry</i>	<i>Finger geometry</i>	<i>Palm</i>	<i>Signature</i>
Level of Accuracy	Very high	Very high	High	High	High	High	High	High	High
Ease of use	Medium	Low	Medium	High	High	High	High	High	High
Vulnerability to fraud	Very high	Very high	Medium	High	Medium	High	High	High	Medium
Intrusive for human beings	Medium	Medium	High	Medium	High	High	Medium	Medium	Very high
Long-term stability	High	High	Medium	High	Medium	Medium	Medium	High	Medium
Industry standards	-	-	-	ANSI/NIST Data Interchange & FBI Image Compression Standards	Speaker Verification API (SVAPI)	-	-	See finger scanning	-
Factors that may affect performance	Glasses worn by end user	-	Poor lighting, aging of face, glasses, facial hair	Dry, dirty or damaged finger images; age, gender, and race of end-user	Background and network noise, colds, and other factors can change the voice	Diseases such as arthritis and rheumatism in end-users	See Hand Geometry	Dry, dirty, or damaged palm images; age, gender, and race of end-user	Illiteracy; signatures that constantly change or are easily imitated

### **Deciding When to Apply Biometrics, and What Should Be Considered?**

Of course, investigating various existing biometrics systems and products is mandatory. Besides this, there are still many questions that should be answered. What kind of biometrics system is required? Is it an identification system or a verification system? What are the characteristics of the end-user population? What are the ages, genders, ethnic origins, and occupations of the end-user group? In case something is wrong with the biometrics system, what will be the substitute method? What is the accuracy of the biometrics system? Will the population of the system grow? What does the environment look like? At last, a detailed testing plan must be prepared.

## **4.5 Summary**

Biometric devices will continue to improve, becoming even more accurate and reliable as technology evolves. As biometric technologies are more widely accepted, the proliferation of applications should multiply into many phases of our daily activities. The growing interest in the combined use of biometrics and smart cards should also cause an increased growth path for both technologies in the future. Hopefully, in the near future, standards will be available which allow multiple reader technologies from various manufacturers to be utilized within the same system.

## **4.6 References**

- [4.1] International Biometrics Industry Association (IBIA). <http://www.ibia.org>
- [4.2] International Biometrics Group (IBG). <http://www.biometricgroup.com/>
- [4.3] The Biometrics Consortium. <http://www.biometrics.org>
- [4.4] Biometrics Research. <http://biometrics.cse.msu.edu>
- [4.5] S. Liu, M. Silverman: A practical guide to biometric security technology. IEEE Computer Society, IT Pro – Security. [http://www.computer.org/itpro/homepage/Jan\\_Feb/security3.htm](http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm)
- [4.6] East Shore Technologies. <http://www.east-shore.com/>
- [4.7] Fingerprint Technologies. <http://www.fingerprint.com/>
- [4.8] FingerPrint USA. <http://www.fpusa.com/>
- [4.9] Biometrics Reports. <http://www.biometrics.org/REPORTS/CTSTG96/>
- [4.10] The Biometrics Consulting Group, LLC. <http://biometric-consulting.com>
- [4.11] Association for Biometrics (AfB), UK. <http://www.afb.org.uk/>
- [4.12] Australian Biotechnology Association. <http://www.aba.asn.au/>

- [4.13] Financial Services Technology Consortium. Biometrics fraud prevention. <http://www.fstc.org/>
- [4.14] Security Industry Association (SIA). <http://www.siaonline.org/>
- [4.15] The Human Identification Project. <http://www.asti.dost.gov.ph/>
- [4.16] GSA's SmartGov. <http://policyworks.gov/smartgov/>
- [4.17] Biometrics in Human Services User Group. <http://www.bioapi.org>
- [4.18] Biometrics and Security. <http://www.infosyssec.org/infosyssec/biomet1.htm>
- [4.19] A. K. Jain, et al. (eds.) (1998) Biometrics: personal identification in networked society. Kluwer, Boston.
- [4.20] B. Miller (1994): Vital signs of identity. *IEEE Spectrum* 32 (2): 22–30.
- [4.21] D. Zhang (2000) Automated biometrics: technologies & systems. Kluwer, Boston.
- [4.22] D. Zhang (ed.) (2002) Biometrics solutions for authentication in an e-world. Kluwer, Boston.
- [4.23] M. Eleccion (1973) Automatic fingerprint identification. *IEEE Spectrum* 10(9): 36–45.
- [4.24] G. Lawton (1998) Biometrics: a new era in security. *Computer* 16–18.
- [4.25] A. Jain, et al. (1997) On-line fingerprint verification. *IEEE Trans PAMI* 19(4): 302–313.
- [4.26] J.P. Campbell (1997) Speaker recognition: a tutorial. *Proc IEEE* 85(9): 1437–1462.
- [4.27] L. Hong, et al. (1998) Integrating faces and fingerprints for personal identification. *IEEE Trans PAMI* 20(12): 1295–1307.
- [4.28] J. Daugman (1993) High confidence visual recognition of persons by a test of statistical independence. *IEEE Trans PAMI* 15: 1148–1161.
- [4.29] Y. Zhang, D. Zhang (2000) A novel text-independent speaker verification method based on the global speaker model. *IEEE Trans SMC (Part A)* 30(5): 598–602.
- [4.30] D. Sims (1994) Biometrics recognition: our hands, eyes and faces give us away. *IEEE Comput Graphics & Apps*.
- [4.31] J. D. Woodward (1997) Biometrics: privacy's foe or privacy's friend? *Proc IEEE* 85(9): 1480–1492.
- [4.32] A. Davis (1997) The body as password. *Wired*, July Issue.
- [4.33] D. R. Richards (1995) Rules of thumb for biometrics systems. *Security Manage*, October Issue.
- [4.34] G. Lawton (1998) Biometrics: a new era in security. *IEEE Computer*, August Issue.
- [4.35] R. Mandelbaum (1994) Vital signs of identity. *IEEE Spectrum*, February Issue.
- [4.36] M. Golfarelli, D. Maio, D. Maltoni (1997) On the error-reject trade-off in biometrics verification systems. *IEEE Trans PAMI* 19(7): 786–796.
- [4.37] R. P. Wildes (1997) Iris recognition: an emerging biometrics technology. *Proc IEEE* 85(9): 1348–1363.

- [4.38] C. Seal, D. McCartney, M. Gifford (1997) Iris recognition for user validation. *British Telecommunications Engineering* 16.
- [4.39] A. K. Jain, H. Lin, P. Harath, R. Bolle (1997) An identity-authentication system using fingerprints. *Proc IEEE* 85(9): 1365–1388.
- [4.40] A. Jain, H. Lin, R. Bolle (1997) On-line fingerprint verification. *IEEE Trans PAMI* 19(4): 302–313.
- [4.41] A. R. Roddy, J. D. Stosz (1997) Fingerprint features: statistical analysis and system performance estimates. *Proc IEEE* 85(9): 1390–1421.
- [4.42] <http://www.nwfusion.com/research/biometrics.html>
- [4.43] <http://www.veridicom.com/technology/Biometric%20Applications.pdf>
- [4.44] [http://www.iris-scan.com/iris\\_recognition\\_applications.htm](http://www.iris-scan.com/iris_recognition_applications.htm)
- [4.45] <http://www.biometritech.com/features/deploywp4.htm>
- [4.46] <http://www.vanguard-fire-security.com/security.htm>
- [4.47] <http://www.fcw.com/geb/articles/2002/0311/web-face-03-04-02.asp>
- [4.48] [http://hydria.u-strasbg.fr/~norman/BAS/intro\\_to\\_biometrics.htm](http://hydria.u-strasbg.fr/~norman/BAS/intro_to_biometrics.htm)
- [4.49] [http://www.computer.org/itpro/homepage/jan\\_feb01/security3b.htm](http://www.computer.org/itpro/homepage/jan_feb01/security3b.htm)



## 5 Smart Cards and Applications

Weidong Kou<sup>1</sup>, Simpson Poon<sup>2</sup>, and Edwin M. Knorr<sup>3</sup>

<sup>1</sup> University of Hong Kong  
Pokfulam Road, Hong Kong

<sup>2</sup> School of Information Studies  
Charles Sturt University, Australia

<sup>3</sup> Department of Computer Science  
University of British Columbia, Canada

### 5.1 Introduction

A smart card is a plastic card with an embedded integrated circuit (IC). A smart card resembles a credit card, with the difference being a chip and (for most smart cards) its metal contacts. A host computer or smart card terminal runs the off-card application and communicates with the card's embedded chip to exchange data and commands. The plastic card usually conforms to physical standards for bank/credit cards, and is a convenient and acceptable way of carrying the chip. Smart cards may contain a microprocessor, random access memory (RAM), read only memory (ROM), and electrically erasable programmable read-only memory (EEPROM). The first patent for a smart card was issued in 1974 to Roland Moreno of France.

Depending on how communication takes place, the smart card can be either contact-based or contactless. For contact-based smart cards, communication takes place through the contacts. The visible contacts cover an area approximately 1cmx1cm (i.e., 100 mm<sup>2</sup>); however, the chip itself is usually no more than 25 mm<sup>2</sup>. For contactless smart cards, communication takes place through wireless transmission.

Smart cards have some type of non-volatile storage, and can be classified according to whether or not they have a microprocessor. Over half of the smart cards in circulation today do not contain a microprocessor. Such cards are referred to as memory (smart) cards, and are used primarily for storing information or value. These cards have been successfully used for years (primarily in Europe

and Asia) for electronic payment in pay phone, vending, and transportation applications, among others.

Smart cards with an embedded microprocessor are sometimes thought of as truly “smart” cards - at least in terms of processing functionality. These cards can perform very reliable security functions, such as authentication, digital signatures, and encryption. A microprocessor allows a smart card to operate independently of a host computer or smart card terminal, thereby enabling essential security operations, such as the creation of a digital signature without the signing key ever leaving the card. These smart cards play a crucial role in information and network security, digital identification, order authorization, and payment processing in electronic commerce applications.

Smart cards have a huge market potential. Currently, billions of smart cards are in use. According to a 1998 report by Gemplus and the Smart Card Industry Association, approximately 805 million smart cards were issued in 1996, and 2.8 billion cards were forecast for 2000. A more recent report from SchlumbergerSema, however, reports that only 1.8 billion cards were issued worldwide in 2001, and furthermore, this figure represents only a 1% increase from 2000. This mild increase stands in contrast to the annual 20% growth rate in recent years, but SchlumbergerSema predicts increases of 7% and 10%, respectively, in 2002 and 2003. Much of this growth is expected to be driven by smart-card-enabled PKI applications, including wireless applications, national ID programs, and network access for enterprise applications.

In terms of applications, prepaid phone cards are still the most popular, followed by mobile communications, and banking. Table 5.1 shows the usage of smart cards. Multi-application cards include applications such as healthcare, loyalty points, secure remote access, and “electronic purse” applications for electronic payment. On electronic-purse cards, real money is represented as a string of bits, and is exchanged among parties.

Table 5.1 Smart card breakdown<sup>1</sup>

<b>By Application</b>	<b>2000 actual</b>	<b>2003 estimate</b>
Pay Phones	1,040,000,000	990,000,000
Mobile Communications	450,000,000	550,000,000
Banking	120,000,000	220,000,000
Others	180,000,000	357,000,000
<b>Total</b>	<b>1,790,000,000</b>	<b>2,117,000,000</b>

<sup>1</sup> Source: SchlumbergerSema, March 2002

<b>By Region</b>	<b>2000 actual</b>	<b>2003 estimate</b>
Europe, Middle East, Africa	895,000,000	974,000,000
Asia Pacific	519,000,000	656,000,000
Latin America	340,000,000	402,000,000
North America	36,000,000	85,000,000
Total	1,790,000,000	2,117,000,000

<b>By Technology</b>	<b>2000 actual</b>	<b>2003 estimate</b>
Memory Cards	1,126,000,000	1,155,000,000
Microprocessor	664,000,000	962,000,000
Multiapplication (of which are Java Cards...)	115,000,000 (53,000,000)	530,000,000 (336,000,000)

## 5.2 Fundamentals of Smart Card Systems

A smart card *system* is a distributed computing system consisting of smart cards, smart card readers, smart card operating systems, file systems, and communication interfaces. In this section, we describe the components of a typical smart card system.

### 5.2.1 Smart Cards

Depending on chip type and method of communication with the reader, smart cards can be classified into different categories. First, the chip can either be a memory chip or a microprocessor. Second, smart cards can communicate with readers either using the contacts on the cards, or wirelessly (in the case of contactless cards). In the latter case, radio waves are used to energize and communicate with the chip. Third, smart cards come in at least two sizes: the size of a standard bank/credit card, and a smaller size for a subscriber identification module (SIM) for global system for mobile communications (GSM) cellular phones.

#### Memory Chips

Smart card memory chips are designed in accordance with their intended applications. The types of memory used for smart cards include:

- Random access memory (RAM):  
This type of memory is used as a short-term work area. Memory contents are lost when the power is switched off.

- Read-only memory (ROM):  
This type of memory is used for storing software.
- Erasable programmable read-only memory (EPROM):  
This type of memory can only be changed once, and is often used in pre-paid service cards, such as telephone calling cards that count off minutes of use. (For telephone applications, the cards can be discarded when there are no units of value left because the cards cannot be reloaded with value.)
- Electrically erasable programmable read-only memory (EEPROM):  
This type of memory can store programs or data. The contents of the memory are preserved when power is switched off, and the memory can be modified up to about 100,000 times.

The architecture of a memory chip varies, depending on the intended application. An example is shown in Fig. 5.1. In particular, a smart card memory chip may contain the following data for communication with the reader:

- Smart card issuer
- Smart card serial number
- Counter logic
- Secret codes or keys

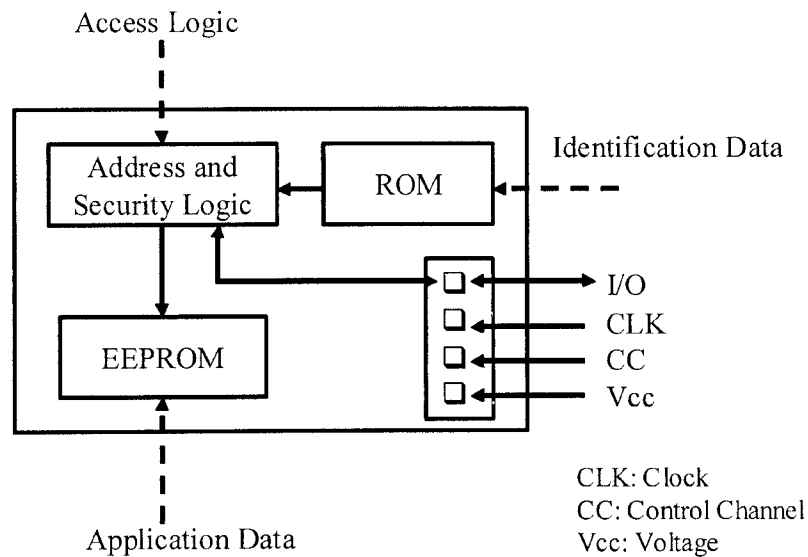


Fig. 5.1 Architecture of a memory smart card

### Microprocessor Chips

As shown in Fig. 5.2, microprocessor chips for smart cards contain a CPU, RAM, ROM, EEPROM, I/O control port, and operating system. The CPU is usually an 8-bit processor, which is a smaller and slower version of the CPU used in a typical PC; however, the smart card's CPU could be a 16-bit, 32-bit, or 64-bit version instead. Besides the processor, there are memory components: ROM, which contains the chip's operating system; RAM, which serves as the processor's working memory; and EEPROM, which stores data and program code. Typically, with respect to memory size, RAM is in the range of 256 bytes to 1 KB, ROM is in the range of 16~32 KB, and EEPROM is in the range of 1~16 KB. The connection to outside the chip is via the I/O control port.

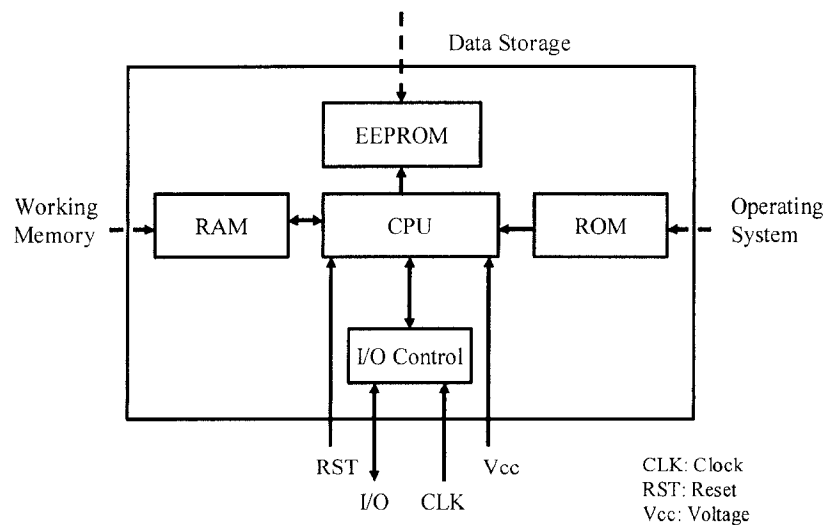


Fig. 5.2 Architecture of a microprocessor smart card

A smart card chip may have an arithmetic co-processor for cryptographic functions. Some chips also have a random-number generator that can facilitate mutual authentication and secure electronic payment.

### Contact Smart Cards

Contact smart cards make their physical interface with a smart card reader through an eight-pin contact, as defined in Part 1 of the ISO 7816 standard. These pins are defined as I/O, reset, clock, ground, Vpp (programming voltage), etc. Note that

the contacts may become dirty, worn (through use), or damaged (intentionally or unintentionally). Also, hackers use the contacts to launch security attacks. Contactless smart cards are a workaround to most of these problems.

### **Contactless Smart Cards**

Contactless smart cards communicate with a card reader through an antenna embedded in the card. Many such cards have approximately a 10-cm range, but there are systems that work up to a distance of 1 m. The antenna on a smart card can be quite small (e.g., less than 1 cm in diameter). Through an antenna, a contactless smart card can collect its power from a radio frequency (RF) field generated by the card reader. The RF field also transfers information to and from the card.

Since there is no need to insert a contactless smart card into a card reader, such cards can be more convenient. A successful contactless smart card application for public transportation is the Octopus card in Hong Kong, which we describe in detail later in this chapter. Another successful contactless application is access control (via employee badges).

### **5.2.2 Smart Card Readers**

A smart card reader is a device that sets up a communication link or interface between a smart card and a host, such as a PC. Smart card readers are also known as *card acceptance devices* (CADs). They interface with a host through RS232 serial ports, parallel ports, USB ports, PCMCIA slots, infrared IRDA ports, or floppy disk slots. They can also be integrated with a computer keyboard, or embedded into various devices or terminals, such as bank ATMs, kiosks, vending machines, TV set-top boxes, cellular phones, personal digital assistants (PDAs), or handheld computers.

Since a smart card contains no independent power source or clock signal to drive its processor, one of the functions that a reader needs to perform is to provide the card with both power and a clock. In the case of a contact smart card, this is done via the contact pins. In the case of a contactless smart card, the task is accomplished via the embedded antenna.

Depending on whether the smart card is a memory or a microprocessor card, the reader either acts as a translator between the host and the card, or it directly passes commands from the host to the card. For a memory smart card, the reader views the physical card structure to get the exact data address and perform the translation. For a microprocessor smart card, the operating system and logic stored on the smart card directly interpret the commands that have been passed by the reader from the host to the card.

Smart card readers can be classified into two categories: stationary readers and mobile readers. Stationary readers have a permanent connection to the host and are usually powered by the host through the data interface. The host drives the reader and the card, and is responsible for all signaling functions, including initialization and communication. Mobile readers, on the other hand, are stand-alone devices that are battery-powered. A mobile reader initializes communication with the smart card. The host is only concerned with communication with the reader (and not with the smart card).

**5.2.3 Smart Card Operating Systems**

A smart card operating system typically contains a few thousand bytes of code, and it loads, operates, and manages one or more applications on the card. Unlike DOS, Windows, Unix, or Linux, smart card operating systems are tiny and do not support the rich functionality that these other operating systems provide, such as providing user interfaces or controlling external resources other than the I/O port.

A smart card operating system allows a card reader to send a command to a smart card. The card executes the command, returns a result (if appropriate), and waits for the next command.

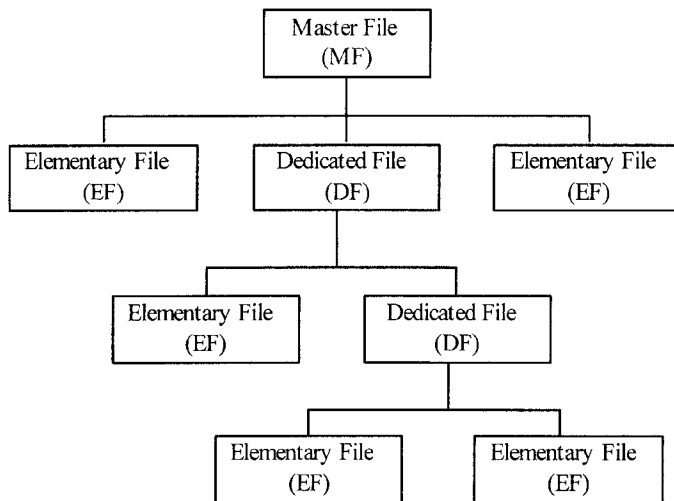


Fig. 5.3 A hierarchical file system for a smart card

Different smart card manufacturers offer different operating systems. Throughout the 1980s and 1990s, various smart card operating systems have been developed for specific applications, such as a data repository. These operating systems

are written into ROM. They are proprietary and specific to a smart card chip. A hierarchical file structure, such as that shown in Fig. 5.3, has been used in these systems. Here, the master file serves as the root of the hierarchical file structure, a dedicated file is a directory, and an Elementary File is a leaf node.

As a smart card evolves from a data-storage device to a transaction device, a hierarchical file structure may not be the best choice. New data structures have been created using the industry standard “Create Table” and “Create View” SQL statements (i.e., from the database community). The key advantage is to allow different applications to share a common data structure.

In addition to sharing, it is important for an application not to read or overwrite another application’s data, without that other application’s consent. This means that the smart card operating system must control memory allocation for each application (e.g., for loading or retrieving data from RAM and EEPROM storage areas).

Given that a smart card application may need to be updated after a smart card is issued, and that various smart card readers may need to access information on the card, new extensions are required for smart card operating systems. Such extensions include an application programming interface (API) and an object-oriented programming language (e.g., Java) that can be used on many different platforms ranging from PCs to hand-held devices.

#### **5.2.4 Communication Interface**

Communication between a smart card and a reader typically goes through a half-duplex physical channel on which the reader and the card can only transmit in turn (i.e., the other party has to be in reception mode). In this section, we examine how communication protocols on top of this half-duplex physical channel are established, and how data is transferred.

When establishing communication between a smart card and a reader, it is always the reader that takes the initiative. The card never transmits data without an external request from the reader. To illustrate, consider a contact smart card. When the card is inserted into the reader, five contacts on the card are electrically activated, and the card automatically executes a power-on-reset. Then, the answer to reset (ATR) is sent to the reader. The reader may optionally send a PTS (protocol type select) request command to the card after it successfully evaluates the ATR, and the card responds to the reader with a PTS-response. Both ATR and PTS are independent of the transmission protocol, and they are used for initialization and for setting various transmission parameters. After initialization, the reader sends the card the first command. The card processes the command and sends a response. This kind of command-response protocol is how the reader and the card communicate.



Communication between the card and the reader takes place serially through a bit-serial data stream. The bit order for converting a byte into the bit-serial data stream must be considered. In the direct convention, the first data bit after the start bit is the lowest in the byte, where the start bit is used for indicating the beginning of each serially transmitted byte. A parity bit is at the end of each byte. One or two stop bits may also be added after the parity bit.

In terms of transmission, a basic question is whether data should be transferred in byte mode or in block mode. In answer to this question, there are two transmission protocols at the data link layer, namely T=0 and T=1 protocols. The T=0 protocol is the asynchronous, half-duplex, byte-oriented protocol, which is covered by the ISO/IEC 7816-3 standard, dominating in Europe and widely used in various smart card systems (e.g., GSM applications). The T=1 protocol is the asynchronous, half-duplex, block-oriented protocol, which is covered by the ISO/IEC 7816-3 Amendment 1 standard. The data structures used in the exchange between the reader and the card in the command-response protocol are called transmission protocol data units (TPDUs).

On top of the data link layer protocols (T=0 and T=1), application-layer protocols can be defined for smart card applications to exchange control and information between the card and the reader. There are two application protocols that have been defined in the ISO/IEC 7816-4 standard. One protocol is for providing a file system for storing and retrieving information on a smart card, and the other is for accessing security services on the card. The former is defined in the form of a collection of functions for selecting, reading, writing, and erasing files, while the latter is defined in the form of a series of security functions. To support these two protocols, the ISO/IEC 7816-4 standard defines data units in the application layer, called application protocol data units (APDUs), which are used for data exchange between the card and the reader.

Fig. 5.4 is a high-level summary of our discussion about the communication model between a smart card and a smart card reader.

Application Layer	ISO/IEC 7816-4 ISO/IEC 7816-7
Data Link Layer	ISO/IEC 7816-3 (T=0) ISO/IEC 7816-3 Amd. 1(T=1)
Physical Layer	ISO/IEC 7816-3 (Contact cards) ISO/IEC 10536-3 (Contactless cards)

Fig. 5.4 Communication model between a smart card and a reader

Before discussing the communication protocols in further detail, let us examine the TPDU and APDU data structures. Fig. 5.5 shows the TPDU data structure for a command with the transmission protocol T=0, which consists of a header and optionally a data section. The header has five fields: a class byte (CLA), an instruction byte (INS), and three parameter bytes (P1-P3), where parameter P3 is a length datum to indicate the length of the data byte transferred to or from the card. The data structure for a response with T=0 consists of an acknowledge byte (ACK), a flow control byte (NULL) to let the reader know that the card is still processing the command and is not yet ready to receive another command, a status return code (SW1), and optionally a return code (SW2) to indicate the amount of data (if the response contains data).

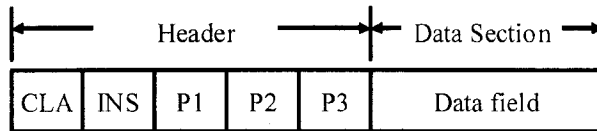


Fig. 5.5 TPDU command data structure with T=0

The transmission protocol T=1 is block-oriented. There are three types of blocks in the T=1 protocol: information block (I-block), receive ready block (R-block), and supervisory block (S-block). Each block contains two mandatory fields (prolog and epilog), and one optional field (information), as shown in Fig. 5.6. The prolog field consists of three bytes: node address byte (NAD), protocol control byte (PCB), and length byte (LEN). The information field contains the application layer's data (APDU) and it may be up to 254 bytes in length. The epilog field contains an error detection code with a length of either 1 or 2 bytes.

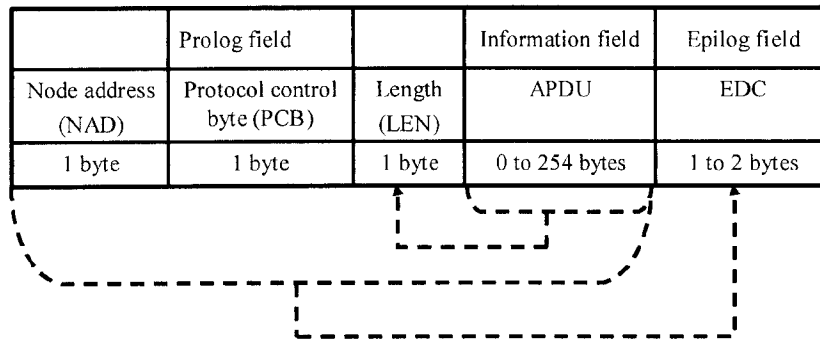


Fig. 5.6 T=1 transmission block structure

There are two APDU data structures: the command APDU structure and the response APDU structure. The command APDU structure consists of a header and a body, as shown in Fig. 5.7. The header includes CLA, INS, P1, and P2 fields. The body may be of variable length or it may be absent (when the data field is empty). The Lc field specifies the length of data sent to the card. The Le field indicates the length of data to be sent back from the card. There are four cases for the command APDU structure:

- Case 1: No data is to be exchanged, and the command APDU structure only contains the header.
- Case 2: No data is transferred *to* the card, but data is transferred *from* the card. The command APDU structure contains the header and the length (Le) of data returned from the card.
- Case 3: Data is transferred *to* the card, but not *from* the card. The command APDU structure contains the header, the length (Lc) of data transferred to the card, and the data field.
- Case 4: Data is transferred both to and from the card. The command APDU structure contains the header, the length (Lc) of data transferred to the card, the data field, and the length (Le) of data returned from the card.

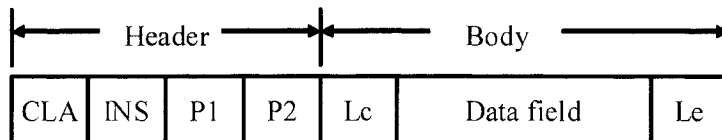


Fig. 5.7 Data structure of an APDU command

The response APDU structure consists of an optional body and a mandatory trailer, shown as in Fig. 5.8. The body contains the data field. The data length is determined in the Le field of the previous command APDU structure. The trailer contains two bytes, SW1 and SW2, which are the designated return codes for the response to the command.

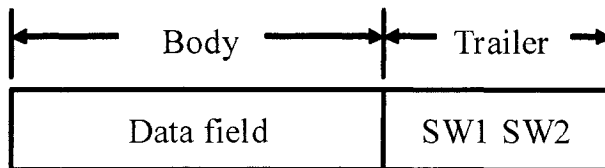


Fig. 5.8 Data structure of an APDU response

### 5.3 Java Card

A Java Card implementation of a smart card application runs programs written in a subset of the Java programming language, in byte-code form. (Java Card technology can also be applied to other resource-constrained devices.) Java Card defines a runtime environment supporting the smart card's memory, communication protocols, security, and application execution. It changes the landscape of the smart card world for the following reasons:

- **Platform independence**  
Applications written for one smart card platform can run on other platforms (from different vendors), provided that those platforms support Java Card technology.
- **Ability to run multiple applications**  
Downloadable Java byte-code enables multiple applications from multiple vendors to be run securely on a single smart card. For example, a single Java Card can be used as an electronic purse, an employee badge (for accessing buildings), a healthcare card, and a telephone card.
- **Ease of upgrades**  
Java Card technology allows the card issuer to: (a) upgrade existing applications on a card, and (b) download new, additional applications to a card.
- **Compatibility with existing standards**  
Java Card technology is compatible with existing smart card standards, such as ISO 7816 and EMV (Europay, MasterCard, Visa).
- **Security**  
The Java virtual machine implements Java-language security policies even though the Java Security Manager class is not supported by Java Card. This means that the level of access to all methods and instances of variables is strictly controlled. Java's "no pointers" feature prevents malicious programs from accessing data in memory.
- **Availability of sophisticated Java application development tools**  
There are a number of integrated Java development tools from leading software vendors such as Borland, IBM, Microsoft, Sun, and Symantec. Java Card developers can choose a tool to create and debug Java Card applications. This is in contrast to traditional smart card application development where a smart card application is coded in assembly language, compiled into machine code, and then burned into ROM. The traditional development method needs a relatively long time to develop and deploy a smart card application, and once the application is deployed it is hard to

make changes. With Java development tools, a Java Card application can be developed and deployed easily and quickly. Furthermore, the deployed Java Card applications can be easily upgraded.

- **Large and growing pool of experienced Java programmers**  
Due to Java's popularity, there is a large and growing pool of experienced Java programmers. Java programmers can easily become Java Card programmers; consequently, the cost of acquiring and training Java Card programmers is minimized.

Due to the resource constraints of smart cards, Java Card only supports some of the features of the Java language (e.g., small primitive data types, 1-D arrays, Java object-oriented features, Java packages, classes, interfaces, and exceptions), but preserves many benefits of the Java language, including productivity, security, robustness, tools, and portability. The Java Card virtual machine is split into two parts: one part running off-card, and the other part running on-card. The assumption is that many processing tasks that require significant resources or that do not have to be executed at runtime can be run on the off-card part of the Java Card virtual machine.

Java Card separates the smart card system and its applications, and uses a well-defined high-level API for application requests for system services and resources. Java Card technology defines a platform consisting of three parts:

- **Java Card virtual machine (JCVM)**  
The JCVM consists of two separate pieces: the Java Card interpreter and the Java Card converter.
  - **Interpreter**  
This is the on-card part of the Java Card virtual machine, providing runtime support for the Java language model. The interpreter executes Java byte-code instructions and Java applets, controls memory allocation and object creation, and enforces runtime security.
  - **Converter**  
This is the off-card part of the Java Card virtual machine. The converter loads and preprocesses all the Java class files that make up a Java package and converts the package to a converted applet (CAP) file. It also verifies the Java-class load images, checks for violations, initializes static variables, optimizes the byte-code, and allocates storage.
- **Java Card runtime environment (JCRE)**  
The JCRE consists of the Java Card system components that run inside a smart card, and serves as the operating system of the smart card. It manages card resources, executes Java applets, and ensures on-card system

and applet security. It is also responsible for network communication. JCRE has three layers, as shown in Fig. 5.9. The bottom layer contains the JCVN and the native methods that support the low-level communication protocols, memory management, and implementation of cryptographic functions. The middle layer contains system classes that manage transactions and communication, and control applet creation, selection, and deselection. The upper layer contains framework classes, industry-specific extensions, and the installer. The framework classes define the APIs that make the creation of an applet relatively easy. The industry-specific extensions are the add-on libraries supplied by specific industries or businesses to provide additional services. The installer is used for easily upgrading existing applications and for downloading new applications after the smart card has been issued.

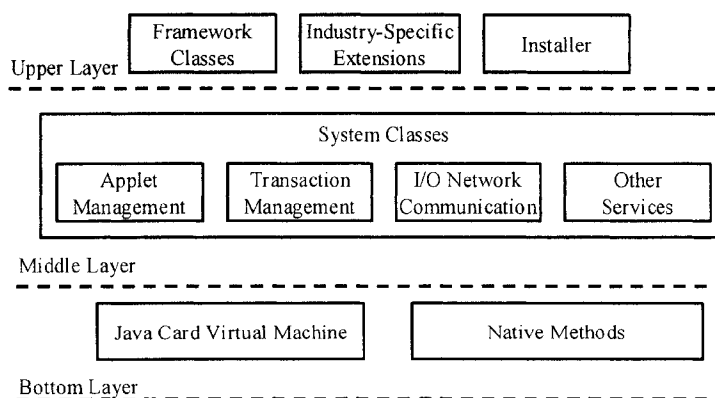


Fig. 5.9 Three-layered Java Card runtime environment

- Java Card API**  
 The Java Card API defines the calling conventions for programming smart card applications, by which the applications can access the JCRE and native methods. It specifies a subset of Java that is tailored for use in smart cards and other devices with limited memory. The Java Card API consists of four packages: three are core packages, and one is an extension package. They are `java.lang`, `java.framework`, `javacard.security`, and `javacardx.crypto`. These packages contain a set of customized compact classes supporting smart card standards, such as ISO 7816, and providing cryptographic services. The significance of the Java Card API is that it frees smart card developers from the development limitations (e.g., a proprietary assembly language) imposed by specific smart card manufacturers.

### 5.4 Smart Card Standards

In order for smart cards to be used en masse in the marketplace, interoperability between smart card systems from different vendors must be supported. Thus, there must be a standard upon which every vendor agrees. A standard is an open specification that lays down the rules, guidelines, or requirements that (a) have been proposed and agreed to, with the consensus of many interested parties, and (b) have been adopted by a recognized standards organization, such as the international organization for standardization (ISO) or the international electrotechnical commission (IEC).

Many standards organizations, such as ISO, IEC, European Telecommunications Standards Institute (ETSI), and American National Standards Institute (ANSI), have been actively involved in smart card standardization efforts. As a result, a set of standards on smart cards has been produced. Some of these standards are listed in Table 5.2. These standards play a key role in promoting the interoperability of smart card systems from different manufacturers and vendors.

Table 5.2 Selected smart card standards

Standard	Subject
ISO/IEC 7810	Physical characteristics
ISO/IEC 7811	Recording techniques: magnetic stripe & embossing
ISO/IEC 7812	Numbering system
ISO/IEC 7813	Financial transaction cards
ISO/IEC 7816	Contact cards
ISO 10373	Test methods
ISO 10536	Contactless cards
ISO 14443	Remote coupling communication cards

ISO/IEC 7810 defines the physical characteristics of smart cards, including visual and physical durability, embossing, and the location of a magnetic stripe. The information that identifies the cardholder and supports the transaction via the card may be conveyed via either a magnetic stripe, or a chip. ISO/IEC 7811 defines how to encode the information. ISO/IEC 7812 specifies how to construct the card identification number, which is up to 19 characters long and has three components: issuer ID number, individual account ID number, and check digit. ISO/IEC 7813 defines the location of embossed characters on the card. ISO/IEC 7816 is for contact smart cards, and specifies the following distinct parts:

- Physical characteristics (Part 1)
- Dimensions and locations of contacts (Part 2)

- Electronic signals and transmission protocols (Part 3)
  - Protocol type T=1, asynchronous half-duplex block transmission protocol (Part 3, Amendment 1)
  - Revision of protocol type selection (Part 3, Amendment 2)
- Inter-industry commands (Part 4)
- Numbering system and registration procedure for application identifiers (Part 5)
- Data elements for interchange (Part 6)
- Query language commands (Part 7)
- Security architecture (Part 8)
- Inter-industry enhanced commands (Part 9)
- Synchronous cards (Part 10)

ISO 10373 defines the test methods for smart cards. ISO 10536 covers contactless smart cards and defines a close-coupled card having a range up to 10 cm. It comprises the following parts:

- Physical characteristics (Part 1)
- Dimension and locations of the coupling elements (Part 2)
- Electronic signals and reset procedures (Part 3)
- Answer to reset and transmission protocols (Part 4)

ISO 14443 is a specification for contactless cards that changes the contact description to an antenna, and defines the protocol for communication over the air. It consists of the following four parts:

- Physical characteristics (Part 1)
- Radio frequency interface (Part 2)
- Transmission protocols (Part 3)
- Transmission security features (Part 4)

In addition to these ISO/IEC standards, there are smart card industry de facto standards and other regional standards. For example, the following standards define the operation of a smart card for various applications.

- EMV: This specification for payment systems based on ISO 7816 defines the content, structure, and programming of chip-based payment cards. It defines how smart cards exchange information with a payment terminal (e.g., PIN checking), and how security is enhanced by preventing the reading of certain low-level information.
- PC/SC: The PC/Smart Card architecture is an open architecture defined by various smart card and PC operating-system vendors including CP8 Transac, Schlumberger, Siemens Nixdorf, HP, and Microsoft. It defines a general-purpose architecture for multiple applications to share smart



card devices attached to a system through low-level device interfaces, device-independent APIs, and resource management.

- OpenCard: The Open Card Framework (OCF) specifications are open specifications allowing applications to be independent of the specific design of smart cards from different manufacturers. The difference between Open Card and Java Card is that Open Card runs Java on the host or terminal side, whereas Java Card runs (a subset of) Java on the smart card itself.
- ETS 300 608: This is a specification from the European Telecommunications Standards Institute defining a smaller-sized smart card (SIM card) to fit into GSM phones (GSM 11.11).

## 5.5 Smart Cards and Security

Smart cards are excellent vehicles for implementing security. They are a crucial part of security infrastructures. In the following sections, we examine the role of smart cards in key management, digital signatures, identification, authentication, and authorization.

### 5.5.1 Smart Cards in Key Management

Key management is essential for security, and is the hardest part of security. Secure electronic commerce applications rely on secure algorithms or protocols involving keys, and the key information must be kept secret. It is not easy to invent a new security algorithm/protocol that will be adopted widely for electronic commerce applications; it is even harder to keep key information secret.

There are millions of users of electronic commerce applications. It can be quite challenging to create, distribute, store, retrieve, and destroy keys for millions of users. Although an asymmetric cryptographic system, as discussed in previous chapters, can be used to solve the key management problem, a problem remains about how to keep one's private key confidential. Smart cards offer a solution to this problem. An individual's private key can be stored on a smart card with the aid of a PIN. The PIN can be used to generate a key to encrypt the private key. Then, if the smart card is lost or stolen, no one will be able to access the private key without knowing the PIN.

### 5.5.2 Smart Cards in Digital Signatures

A digital signature is a piece of data that is created with a signer's private signature key and is a function of the message being digitally signed. To generate a

digital signature, a private signature key is required. As we discussed in the last section, smart card can be used for storing this private key.

A digital certificate is an electronic set of credentials for a signer, issued by a trusted authority called a certificate authority (CA). This confirms both the signer's identity and their public key. In some digital-signature implementations, a digital certificate of the signer is required as an appendix to the signed message. This makes the verification process simpler, since the certificate accompanies the message. In this case, it is no longer necessary to obtain the signer's digital certificate from an X.500 directory in a public key infrastructure. Smart cards can be used to store one's digital certificate in addition to one's private signature key.

### 5.5.3 Smart Cards in Identification

Identification is essential to secure electronic commerce. Smart cards can be used as a means of identification, in place of other forms of ID, such as passports. Various governments have expressed interest in national ID cards, including Malaysia, Hong Kong, and Singapore. Such cards can be used to securely store personal ID, healthcare information, and other data (including financial data), on a single smart card. For example, the Hong Kong Special Administration Region government plans to issue citizen identification cards, that is, smart cards containing personal identification information.

As mentioned in Section 5.5.1, if an individual's smart card containing encrypted or protected information is lost or stolen, no one else will be able to use it. In this regard, smart cards can be a better form of identification than passports. The use of a smart card for identification can provide more efficient processing of individuals at international border checkpoints.

The use of smart cards can also reduce fraud in healthcare and welfare systems. These two systems are well known for abuse and high costs (e.g., due to claims by ineligible recipients, or due to multiple claims in one or more jurisdictions). Banks and credit card companies can save millions of dollars in losses due to fraud, again by using smart cards as a form of cardholder identification.

### 5.5.4 Smart Cards in Authentication

As discussed in Chapters 2-3, authentication is the process by which an entity's identity is verified. Authentication is typically based one of the following three criteria:

- Something a person knows, such as a PIN or password
- Something a person possesses, such as a smart card

- Something a person uniquely has and cannot easily change, such as a fingerprint, iris image, facial image/structure, voice pattern, etc.

Smart cards can utilize all three of these criteria for authentication. First, a smart card can have a PIN that is only known to the owner of the card. Second, like a bank (ATM) card, each smart card has a unique serial number. Third, unlike a typical bank card, a smart card can store much more information, including information about fingerprints, iris images, etc., that serve to uniquely identify the cardholder (see Chapter 4). Such biometric information can be used to achieve a very high level of security.

Besides authentication via a PIN and the presence of the card, third-party authentication can be performed (either locally or remotely) using a private signature key stored on a smart card. To authenticate the cardholder, the cardholder's digital signature may be verified using a signature-verification process via a third party (i.e., a certificate authority). This third-party authentication is extremely useful for electronic commerce conducted over the Internet.

#### 5.5.5 Smart Cards in Authorization

In electronic commerce, the authorization of a purchase or of a payment for the purchase is required, which can be carried out using smart cards. In the business-to-consumer (B2C) e-commerce applications, the *secure electronic transaction* (SET) protocol (see Chapter 10 for the detailed information about SET) can be used for authorization. In the business-to-business (B2B) e-commerce applications, if the dollar amount of the order is high, multiple levels of authorization may be required. For example, the order may have to be accompanied by the digital signature of the chief financial officer (CFO). To enable secure authorization, a smart card is an ideal tool because a given smart card is unique to the CFO, and no other individual will be able to create the CFO's digital signature. Hence, the likelihood of someone creating a bogus purchase order is minimized.

Smart cards can also be used to implement a hierarchical security scheme for access control, whereby certain individuals within a company are permitted to modify (i.e., add, update, or delete items from) a purchase requisition before it is sent for authorization. This gives authorized individuals the ability to override details on a purchase requisition. Digital certificates can be used to authenticate these individuals.

#### 5.5.6 Summary of Smart Cards and Security

A smart card can be issued to an authorized person and be carried around by that person. The significance of smart cards is that they can be used to securely store

the private keys, the digital certificates containing the public keys, and the cryptographic algorithms. Given that a private key never leaves the smart card, and the cryptographic algorithms on the card are used for security purposes, no third party can intercept the private key by listening to the communication between the card and the reader. In addition, the private key on the card can be protected using a PIN. This enables only the authorized person to make use of the private key for security purposes. The smart card system can even prevent further use of the card by locking out the card after a few unsuccessful PIN attempts.

## 5.6 Smart Card Applications

Smart cards have been widely adopted for many applications throughout the world, but especially in Europe and Asia Pacific. Typical smart card applications include:

- Electronic payment
- Access control
- Telecommunications
- Healthcare
- Transportation
- Identification

### 5.6.1 Electronic Payment

Smart cards play an important role in payment processing in electronic commerce. They can be used to store and process “value” or digital money, and they can be used to add an additional level of security to a credit card or debit card.

A *stored value* smart card cannot be reloaded, and is issued with some fixed amount of value or money (e.g., \$20). As a user purchases goods or services with the card, the monetary value on the card is gradually decremented. Stored value cards have limited hardware functionality and do not contain a microprocessor. The card is decremented by a host application that interfaces with the smart card through a card reader.

An *electronic purse*, on the other hand, is a reloadable smart card. It contains a microprocessor, not only to perform monetary calculations but also to securely store the digital money, to authenticate the host application, and to perform secure communication with the host. A PIN can be used to “lock” the funds on a card to prevent other people from using the card. A Mondex card is an example of an

electronic purse. Mondex digital money can even be exchanged between two smart cards belonging to family or friends, using a device called an electronic wallet.

To prevent a hacker from counterfeiting digital money, it is essential that the smart card guard against unauthorized access. Increases and decreases in monetary value must only take place with accepted host applications, using accepted protocols. Digital certificates are required used to authenticate the host and the smart card.

Not only can smart cards be used in credit card or debit card payment processing, they can be used to write digital signatures for electronic cheques. Electronic cheques are based upon a bank account debit system, and are paperless cheques that can be sent electronically from one entity to another. The receiving entity can endorse the cheque via another digital signature, and e-mail it to a bank.

Finally, we note that privacy is an integral part of payment processing. Smart cards can facilitate privacy through digital signatures or the use of anonymous digital money.

#### **5.6.2 Access Control**

Smart cards can be used to facilitate authorization to physical or logical sites and resources. For example, smart cards can be used in corporate, government, and military environments for physical access control to buildings, rooms, and parking lots. In addition, smart cards can be used for controlling access to, and operation of, designated physical assets, such as:

- Machines
- Vehicles
- Computer equipment
- Telecommunication equipment
- Laboratory research equipment
- Dangerous arms
- Other equipment

There is great potential in employing biometrics in ID cards for strict physical access control of military, government, and financial facilities and assets. Such applications became even more important following the September 11, 2001 terrorist attacks against the United States.

With respect to logical access, smart cards can serve as a form of identification for remote, online access to workstations, files, databases, and networks. Smart cards can be used to implement security using biometrics, without the need for a central, online database. In particular, they can replace many USERID/password

scenarios with automated equivalents, and can provide a very high level of security. For situations where individuals are often working from different terminals, smart card solutions for network access are particularly attractive. Network security will become increasingly important for the Internet.

### **5.6.3 Telecommunications**

Smart cards have been used in telecommunications for years. Typical applications include payment cards for public telephony, and subscriber identity modules (SIM) cards for GSM mobile communications.

Advantages of using smart cards for public telephony include reduced costs of operation since there is no need to collect cash, and theft deterrence (i.e., there is no money available to be stolen).

The use of SIM cards in mobile telephony has enhanced security of GSM because with SIM cards, user authentication, integrity, and confidentiality of voice and data can be provided.

### **5.6.4 Healthcare**

Smart cards are used in healthcare in various ways, including facilitating registration/information in emergency-care situations. For example, in an emergency, a doctor other than the patient's regular physician can access the patient's health information (e.g., blood type, allergies, medicines, special needs, contact information).

Medical insurance companies like smart cards because smart cards can provide information about a patient's insurance eligibility and coverage. They can also be used in an electronic claim submission procedure since both insurance data and patient information can be read and verified from the smart card.

Smart cards are good vehicles for controlling healthcare costs by preventing fraud, especially in public healthcare systems where there may be no good way of verifying eligibility for medical services. Some states or provinces (e.g., British Columbia, Canada) have far more healthcare-benefit cards (not smart cards) in circulation than there are people in the population.

Electronic prescriptions with the physician's digital signature can be stored on smart cards, thereby reducing errors or misunderstandings, minimizing potential drug interactions, and reducing fraud (e.g., some patients visit many physicians, or forge prescriptions, in order to obtain drugs for resale). Healthcare professionals can also use smart cards to control access to unattended workstations in hospital wards.

### 5.6.5 Transportation

Smart cards have been successfully deployed in transportation applications in many cities, including Hong Kong and Shanghai in China. These applications include:

- Drivers' licenses
- Parking permits
- Taxi payments
- Local public transportation
- Train and air travel
- Electronic toll collection

Transportation is a smart card application that can reach a critical mass of people. In Section 5.7, we will take a close look at Octopus cards in the Hong Kong local transportation fare-collection system.

### 5.6.6 Identification

Smart cards are emerging as an excellent tool for personal identification in corporate, government, and university applications. Many organizations are using, or plan to use, smart cards as employee badges for multiple purposes. As mentioned previously, some nations are in the process of deploying smart cards as national identification cards.

In many university campuses, all-purpose student ID cards have been used for various purposes, including electronic payments for applications such as:

- Vending machines
- Laundry machines
- Photocopiers
- Meal payments in cafeterias

These student cards can also be used for identification or access in the following applications:

- Course registration
- Student union or club activities
- Libraries
- Athletic facilities
- Medical care

## 5.7 A Case Study in Smart Cards: Hong Kong's Octopus Card

### 5.7.1 The Rise of the Octopus Card

The history of the Octopus card started in June 1994 when Hong Kong's five major public transportation operators, namely, Mass Transit Railway Corp. (MTRC)<sup>2</sup>, Kowloon-Canton Railway Corp. (KCRC)<sup>3</sup>, Kowloon Motor Bus Company (KMB), Citybus Ltd., and the Hong Kong and Yaumatei Ferry systems (HKF), formed a joint venture company, Creative Star Limited (CSL), to develop an automated fare collection system based on contactless smart cards. The fare collection contract, valued at US\$55 million, was awarded to ERG Australia Limited and its subsidiary AES Prodata, which subsequently awarded the contactless card portion of the contract to Sony and Mitsubishi Corporation. These contactless, reloadable smart cards, known as Octopus cards, were introduced to the general public in September 1997.

An estimated 10 million passenger journeys are made each day on Hong Kong's wide variety of public transportation services. According to a 1998 report by Industry Canada, the Creative Star Octopus System, when launched, was the largest, integrated, contactless, smart card, fare collection system in the world, and accounted for approximately US\$13 million<sup>4</sup> in daily transactions.

Here is how the system works. Each of the operators' computer networks is linked to the Creative Star Clearing House system, which in turn apportions revenue to the operators and deposits funds into the appropriate bank accounts. In mid-2000, there were 6.5 million cards in use, with millions more to follow. Users have the ability to reload their cards with cash (HK\$100 is a typical amount). Cardholders can reload their cards in any MTRC and KCRC station, as well as in any of the 368 7-Eleven convenience stores within Hong Kong. Octopus cards can also be used for other kinds of applications, such as purchasing food or merchandise, and even serving as an employee badge (Leong, 2000).

In 1998, Creative Star negotiated with Mondex and VisaCash to incorporate an electronic-purse function into its originally closed system, with the MTRC still owning a 67.8% stake in Creative Star.

---

<sup>2</sup> MTRC is the metropolitan underground railway system in Hong Kong.

<sup>3</sup> KCRC is an electric railway system that connects the Kowloon peninsula to the New Territories.

<sup>4</sup> At the time of writing, US\$1 equals approximately HK\$7.8.



### **5.7.2 Debit Cards in the Passenger Transportation Industry**

Although various payment-processing applications already exist for smart cards, transit fare collection requires special considerations to ensure its success (Goldfinger, 1988). We itemize these criteria, modeling them as network goods, as follows.

#### **Deployment and Apprehension**

When smart cards were initially introduced for fare collection, there was some apprehension due to technology “hiccups”, and the fact that passengers had to adjust to a new system. In those cases where an existing system was already in place (e.g., magnetic stripe cards), a smooth and short cutover was required to ensure the success of the smart card deployment. Some technical hiccups and customer apprehension had been experienced in previous smart card pilot studies (e.g., Mondex in Manhattan, New York City, in 1998, although that pilot did not involve the transportation sector). The bottom-line is that customers and vendors demand smooth rollouts; otherwise, they will lose confidence in the new technology and be more resistant to embracing it.

#### **Co-operation Among Linked Fare Systems**

In the case of passenger transportation applications, smart card systems often suffer from incompatibility with other fare systems at either the technology or the business level. At the technology level, vendors using incompatible technologies may develop different kinds of smart card systems that are adopted by different transportation providers. Sometimes, many smart card fare systems are used in one mode of transportation (e.g., buses), but not in another. Sometimes, due to different governing and policy-making bodies, the smart card systems are not integrated, even though there is a logical flow of passengers between two transportation systems (e.g., from trains to buses). And of course, customers are inconvenienced if they need to deal with multiple cards for similar applications.

#### **Contactless Requirements**

As mentioned earlier, the term “contactless” means that a transaction performed using a smart card does not require physical contact between the card and the card reader. In fact, many successful transportation-ticketing systems are contactless, and this is important for a number of reasons (Goldfinger, 1998). The user flow rate in some of these systems can be as high as one million or more per day (averaging 19 users per second). During peak hours, the flow rate can be two to three times the average hourly flow rate for the day. In order to handle such a volume, it is important to make sure that the processing time per user is as short as possible.

The critical delay for processing is often not due to transaction processing time, but due to human activity (i.e., locating or fetching the card, and then placing it into the reader). Slot-based cards require the user to physically place the card into a slot and this is the major source of delay for such systems, especially when customers are carrying bags or packages, and there is a queue of passengers boarding.

### **5.7.3 Analyzing the Success of the Octopus Card**

When the Octopus card was introduced in 1997, there were already smart card systems in use, mainly in the form of debit systems introduced by major credit card companies, namely, VisaCash by Visa International, and Mondex by MasterCard. Both VisaCash and Mondex had two key competitive advantages: a large international customer base, and backing by two of the world's largest credit card companies. Both VisaCash and Mondex were in trials around the world. In Hong Kong, Mondex had just launched a trial of its smart card technology, and the results were positive. Given that the Octopus system was still in its infancy, traditional wisdom would have pointed to the demise of an unproven smart card system targeting a local application (i.e., passenger transportation), especially since a magnetic, debit card system was already in place. However, there were a number of factors that made the Octopus card a success, which we outline as follows.

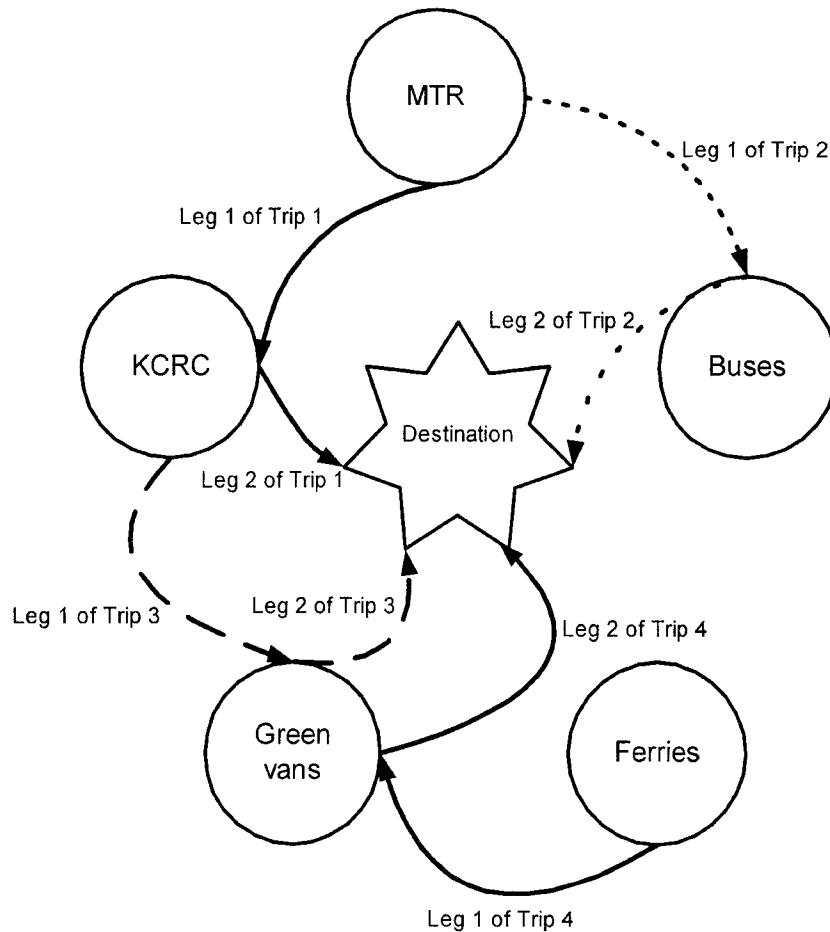


Fig. 5.10 Examples of types of multi-leg trips made in Hong Kong  
(Source: Poon & Chau, 2001)

#### A High-Density City with a Heavy Reliance on Public Transportation

Hong Kong is special in the sense that it has one of the highest population densities in the world, combined with a relatively low rate of private vehicle ownership. The highly congested road system and the high cost of car ownership mean that many Hong Kong people use public transportation for their day-to-day activities. The passenger-transportation sector in Hong Kong includes the MTRC, KCRC, bus companies, ferries, and other auxiliary transit systems, such as the “green vans” (a public, light bus system having designated routes). On average, an indi-

vidual needs to make at least one return trip using the public transport system to go to work, attend school, etc. Given a population of 7.5 million people, if 70% of the population were doing one such trip per day, and spending on average HK\$16.00 (approx. US\$2.00) per return trip, then the daily transactions of the Octopus system would total approximately US\$11 million. Due to the way the Hong Kong passenger transportation system is set up, passengers often need more than one mode of transportation; consequently, the daily transaction volume can be even higher.

### **Sector Wide Adoption with a Common Technological Standard**

Although the use of a stored-value card for local transportation payments has been in place for over two decades in Hong Kong, the diffusion of such an application beyond the Mass Transit Railway Corporation (MTRC) and the Kowloon-Canton Railway Corporation (KCRC) was a recent development. The early stored-value card system used by the railway systems was based on magnetic stripes, and required insertion of the card into a reader slot at a turnstile. For all other modes of public transportation in Hong Kong (e.g., ferries, buses and mini-buses), payments were made by tendering the exact fare using coins into an on-board coin box.

Creative Star Limited was created and backed by the biggest passenger transportation companies in Hong Kong. These companies together operated more than 70% of the passenger transportation business in Hong Kong. Their unanimous adoption of the Octopus card generated an instant critical mass. A critical mass is an essential property for the flow of network goods. This also reflects a spirit of cooperation because the member companies jointly owning Creative Star were direct competitors in some cases.

It has been pointed out that if both the current and new systems coexisted, chances are that the old system would jeopardize the adoption of the new one because of the existing infrastructure and habitual usage (Goldfinger, 1998). In the case of the Octopus card system, the deployment was a quick conversion over a period of a few months, and users had no choice but to use the new system.

As this chapter was written, a sector-wide adoption situation had been achieved with about 40 passenger transportation companies accepting the Octopus card. Almost 7 million cards had been issued by early 2001, of which 1.4 million were sold to children under 18 years of age (Rader and Maghiros, 2001).

### **Captured Market with Reasons for Adoption**

Although coin payment has been well accepted in Hong Kong's passenger transportation system, it has nevertheless been a hassle because of the "exact fare" rule

that requires passengers to have the exact amount ready, usually in the form of coins. Getting change is difficult because there is often no money-change facility near the terminals or bus stops. Sometimes, the only way to get change is from nearby shops or other passengers, neither of which is a welcoming move.

The Octopus card, on the other hand, offers a number of conveniences, especially when considering the contactless property. For those people who have their Octopus cards buried under their belongings in a handbag, for example, there is no need to physically place the card into a reader because the card can be read where it is, providing the card is sufficiently close to the reader. The contactless nature of the card allows for fast scanning. In fact, transaction processing takes less than 300 milliseconds. The fact that there is a captured market of about 7 million cards, with constant use, means that there is a critical mass for this payment infrastructure. More importantly, the clearing and settlement of payments (via HSBC bank, at the time of writing) taking place between Creative Star and the transportation operators, take less time (i.e., less than 24 hours), compared to the considerably longer process involving coin boxes (Leong, 2000).

#### **Fending Off Competition from VisaCash and MasterCard**

When the Octopus card was launched, Visa International and MasterCard were both involved in debit-card trials in Hong Kong. Although both Visa and MasterCard had a much larger customer base and a long track record in the credit card industry, the captured market, contactless nature, and focused application have proven to be important criteria for success. Both VisaCash and Mondex were using contact-based cards, whose transaction times would have been at least as long as it takes for the card holder to place the card into the reader. In the Hong Kong passenger transportation industry, this process was too time-consuming, especially during rush hour. More than 3 million transactions take place per day, during an 18-hour period of operation. During rush hour, however, there might be up to 1.8 million transactions occurring, averaging about 600,000 per hour. Clearly, the contactless nature of the Octopus card and its short transaction time are key reasons for its success.

#### **Expanding to be a Micro-Payment Provider**

The original intent of the Octopus card was to provide a means of payment within the passenger transportation industry. In fact, under the original governance of the Hong Kong Monetary Authority (HKMA) Banking Ordinance, Octopus transactions were to be confined to the transportation and related sectors. However, Octopus can derive up to 15% of the equivalent core transactions from non-transportation sectors. In April 2000, Creative Star Limited was granted a deposit-taking licence by the HKMA, which broadened the card's scope of use (Leong,

2000). Octopus cards can be used for payments at shops in the fast-food sector, kiosks, phone booths, and soft-drink vending machines (Rader and Maghiros, 2001). They can be reloaded not just at MTRC and KCRC train stations, but also at 7-Eleven convenience stores using dedicated devices, and even at the point of transaction if one has an account with the Dah Sing Bank or Standard Chartered Bank. For example, if there are insufficient funds on the card at the time of usage, and the holder has an appropriate credit card from the bank, then the bank will automatically transfer/upload HK\$250 to the Octopus card, without any special handling charge (Dah Sing Bank, 2002). This means that passengers can bypass sales counters and add-value machines. The above reasons make the Octopus card the most mobile-friendly micropayment system in Hong Kong.

#### **5.7.4 Future Developments in the Octopus System**

The Octopus card is in a strategic position to expand its market share, including non-transportation applications. Fig. 5.11 illustrates some of the potential paths for expansion.

##### **All-Purpose Micropayment System**

One potential development path is to have the Octopus card be an organizational charge card. In some organizations, there is a need to have an internal charge card to allow employees to use company resources on a pay-per-use basis. For example, in a university, students have to pay for different services such as photocopying and recreational facilities. The Octopus card is well positioned to take on the role of a university-wide charge card, thereby enabling students to use various resources and pay via an internal Octopus system.

##### **Transaction Services Outsourcing**

The strength of the Octopus system, besides its application in the passenger-transportation industry, is its transaction-clearing system. The high daily transaction volume means Octopus's clearing system rivals that of mid-size banks in Hong Kong (Rader and Maghiros, 2001). The Octopus system, in conjunction with HSBC's Hexagon system, can settle this volume of payments within 24 hours. This very efficient clearing system can be positioned as an outsourcer for other high-volume transaction environments, enabling the Octopus clearing system to become the universal backend for major transaction establishments.

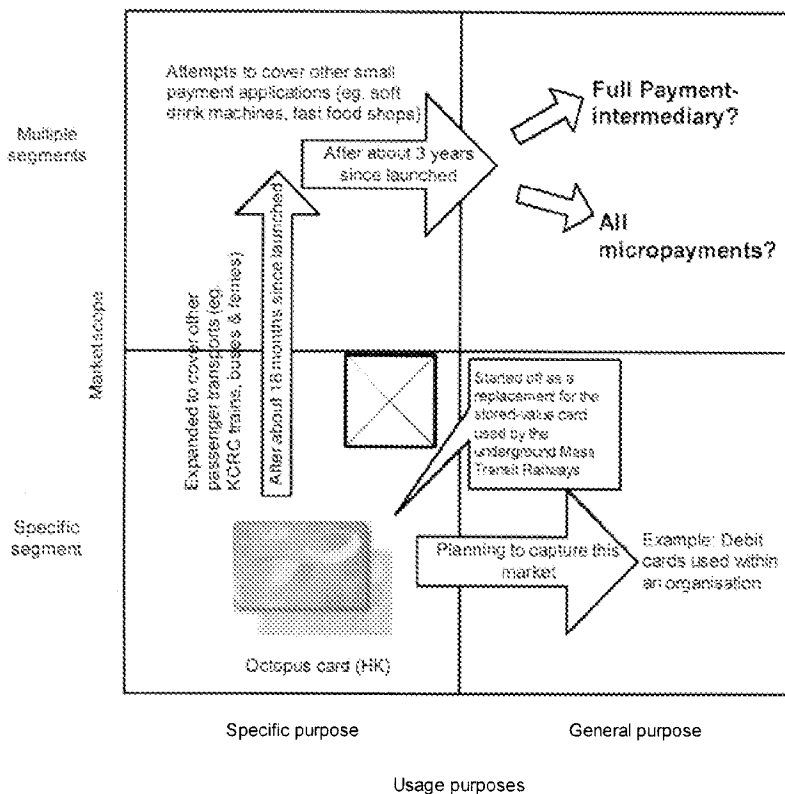


Fig. 5.11 Strategic orientation of the Octopus card and its future (Source: Poon & Chau, 2001)

**5.8 Summary**

In this chapter, fundamentals of smart cards have been introduced, including smart card chips, readers, operating systems, and communication interface. Then, the information of Java Card has been provided. In addition, a set of smart card standards have been presented. The utilization of smart cards in implementing security and possible smart card applications have been discussed. Finally, a case study of Hong Kong’s Octopus cards has been presented.

Smart cards, plastic cards with an embedded IC chip, are excellent vehicles for electronic payment and other applications, such as identification, access control,

telecommunications, healthcare, and transportation. They are also crucial for implementing security. Currently, billions of smart cards are in use, and the market potential of smart cards is huge.

## 5.9 References

- [5.1] Dah Sing Bank: <http://www.dahsing.com.hk/etopup.htm>
- [5.2] W. Ford, M. S. Baum (2001) *Secure electronic commerce* (2nd ed.). Prentice-Hall, New York.
- [5.3] C. Goldfinger (1998) *Economics of financial applications of the smart card: a summary overview*. <http://www.fininter.net/Archives/fasc.htm>
- [5.4] M. Hendry (2001) *Smart card security and applications* (2nd ed.). Artech House, Boston London.
- [5.5] Hong Kong Economic Times (2000) The largest eCommerce network in Hong Kong – the Octopus transaction system. September 27, 2000, IT2–IT3.
- [5.6] W. Kou (1997) *Networking security and standards*. Kluwer, Boston Dordrecht London.
- [5.7] E. Leong (2000) Octopus extends its reach. *FinanceAsia.com*, July 19, 2000.
- [5.8] S. Poon, P. Y. K. Chau (2001) Octopus: the growing e-payment system in Hong Kong. *Electronic Markets* 11(2): 1–10.
- [5.9] M. Rader, I. Maghiros (2001) *Electronic Payment Systems Observatory Newsletter*, No. 5. <http://epso.jrc.es/newsletter>.
- [5.10] B. Schneier (2000) *Secrets and lies: digital security in a networked world*. Wiley, New York.
- [5.11] Sun Microsystems (2002) *Java Card platform security: technical white paper*. <http://java.sun.com/products/javacard>
- [5.12] The World Bank Group (2002) *The Octopus system* (presentation by the Hong Kong MTR Corporation). <http://lnweb18.worldbank.org/External/lac.nsf/Sectors/Transport/0D8952>
- [5.13] U. Hansmann, M. S. Nicklous, et al. (2002) *Smart card programming*. Springer, Berlin Heidelberg New York.



## **6 Wireless Infrastructure**

Weidong Kou

University of Hong Kong  
Pokfulam Road, Hong Kong

### **6.1 Introduction**

Wireless e-commerce (or mobile commerce) is projected to become a US\$12.4 billion market by 2005 in Asia-Pacific, excluding Japan, according to International Data Corp (IDC). Mobile commerce applications such as mobile banking, email, wireless gaming, and stock trading already are available in the marketplace. For example, NTT DoCoMo's i-mode service in Japan, which provides email, web access, wireless banking, stock information service, flight information, online reservations, news and weather, yellow page service, fortune telling, online games, and digital content retrieval from its partners, in addition to regular cellular-phone functions. DoCoMo was formed in July 1992. It had sales of 4.6 trillion yens in fiscal 2000 year ended by March 31, 2001. It was reported that the subscriber number of the i-mode service exceeded 28 million as of October 2001. We see some countries, for example, Korea, where wireless subscription numbers exceed wired customers. A recent statistical report (October 2001) shows that China now has the largest hand-phone user base in the world, with a total of over 120 million users, or 10% penetration rate. In Hong Kong, over 5 million people out of a total of 7 million have a cellular phone. The penetration rates in European countries are also high. All this evidence shows that the growth of mobile commerce is phenomenal and its potential is huge.

Payment is essential for commerce transactions. Mobile commerce transactions also need to have payment in place. To enable the payment process in mobile commerce, we need to have a wireless infrastructure. In this chapter, we will examine various components of such a wireless infrastructure for e-payment and for mobile commerce in general, including wireless communication infrastructure, wireless and pervasive computing infrastructure including wireless and pervasive devices, wireless application protocol (WAP), and wireless security.

## 6.2 Wireless Communications Infrastructure

The Internet is the basis of the World Wide Web, and is the infrastructure that has taken the current form of e-commerce to center stage in the past few years. The Internet has been an interconnected computer network through cables since it was born more than thirty years ago. The rapid development of wireless technologies means the Internet going through a revolution. The Wireless Internet is emerging. Accessing information anytime and anywhere is becoming a reality. This change sets mobile commerce rolling. The essential part of the advances in wireless technologies is wireless communication infrastructure.

There are three main areas of the wireless communication infrastructure: the transmission and media access, the mobile network, and the mobile services. The transmission and medium access area covers wireless transmission technologies (such as multiplexing and modulation) and medium access technologies (such as TDMA and CDMA). The mobile network area addresses the network system architecture and protocols. The mobile services deal with voice and data services such as mobile-prepared services, mobile voice IP, and international roaming.

In wireless communication, radio transmission takes place via different frequency bands. It starts at several kilo-Hz. It can go as high as over one hundred mega Hz. As there exists interference in the radio transmission, and as radio frequencies are scarce resources, the frequencies used for transmission are all regulated.

In order to ensure low interference between different senders, multiplexing schemes have been introduced in four dimensions: space, time, frequency, and code. The space-division multiplexing is a scheme to ensure that there is wide enough distance between senders to avoid interference due to radio transmissions from the different senders. The time-division multiplexing scheme allows senders to use the same frequency but at different times. The frequency division multiplexing scheme is to subdivide the frequency dimension into several non-overlapping frequency bands. Different senders are assigned to different frequency bands. The code-division multiplexing scheme is relatively new, and it resolves the interference problem by assigning senders to different codes, and the distances between these codes are wide enough to avoid the interference. As the many codes can be designed, the code-division multiplexing scheme offers much more flexibility than the space, time, and frequency division multiplexing schemes do.

In wireless networks there is a need to translate the binary bit stream into an analog signal first. This translation is referred to as digital modulation. There are three basic techniques for digital modulations: amplitude shift keying (ASK), frequency shift keying (FSK), and phase shift keying (PSK). In the ASK technique, the binary values, 1 and 0, are assigned to two different amplitudes. The FSK

technique assigns the two binary values, 1 and 0, to two different frequencies. The PSK technique makes use of shifts in the phase of a signal to present the two binary values, 1 and 0, for example, shifting the phase by 180 degrees when the value of data changes. After digital modulation, wireless transmission requires an analog modulation, which is a technique to shift the center frequency of the base-band signal generated by the digital modulation up to the radio carrier frequency. There are three different analog modulation schemes: amplitude modulation (AM), frequency modulation (FM), and phase modulation (PM). These modulation schemes have been widely used, for example, AM and FM radios.

In wireless communication networks, how to allow a mobile-phone user to access the wireless networks is the problem that the medium-access control technology is meant to resolve. The typical algorithms for the medium-access control include space division multiple access (SDMA), frequency division multiple access (FDMA), time division multiple access (TDMA), and code division multiple access (CDMA). SDMA is a technology for allocating a separate space to mobile users in the wireless network. FDMA deals with allocating frequencies to transmission channels according to the frequency division multiplexing scheme. TDMA is to allocate certain time slots for wireless communications. CDMA is to separate different users through the codes used in the code division multiplexing.

The wireless communication systems are cellular, that is, they are designed as a network of cells. In the center of each cell, there is a base transceiver station (or, simply, a base station) that comprises radio equipment for transmitting and receiving radio signals, including antennas, signal processing, and amplifiers. Each cell has a coverage area. A mobile-phone user may move from one cell to another. This movement is called roaming. The process of switching such a user from one cell to another while the user is engaging a call is referred to as a handoff or hand-over.

The popular wireless communication systems include global system for mobile communications (GSM), general packet radio service (GPRS), and code division multiple access (CDMA) systems. Among them, the most popular one is the GSM system that has been used in more than 130 countries worldwide, including most countries in Europe and Asia, excluding Japan. GSM has initially been developed and deployed in Europe to provide a mobile phone system that offers the roaming service to users throughout Europe. Now, GSM supports the integration of different voice and data services and permits an easy system upgrade to higher data rates. GPRS was designed for data services by providing packet-mode transfer for applications, such as web requests and responses, and it promises to provide users with a high-capacity connection to the Internet. CDMA is a digital spread-spectrum system initially developed by a US-based company called Qualcomm, and it has been standardized by the Telecommunications Industry Association (TIA). The CDMA standard is known as Cellular IS-95.

An example of the wireless communication systems is shown in Fig. 6.1. A mobile station (MS) can be held by either a pedestrian or a motion vehicle. The MS communicates with a base transceiver station (BTS). The BTS is managed by a base station controller (BSC) which is connected to either a mobile service switching center (MSC) or a gateway mobile service switching center (GMSC). The MS information is usually stored in a home location register. The MS information can be static and dynamic. The static information includes the mobile subscriber ISDN number, subscribed services, and the authentication key information. The dynamic information includes the current location area of the MS. When an MS leaves the current location area, to localize a user in the worldwide network, this information needs to be stored and updated in a very dynamic database, which is called visitor location register (VLR). The VLR is associated with a MSC, storing the information of the MS who is currently visiting the location area associated to the MSC. The GMSC connects to the public switched telephone network (PSTN). The operation and maintenance center (OMC) monitors traffic and provides management functions such as subscriber and security management, and accounting and billing. The authentication center (AUC) is to protect mobile user identity and data transmission.

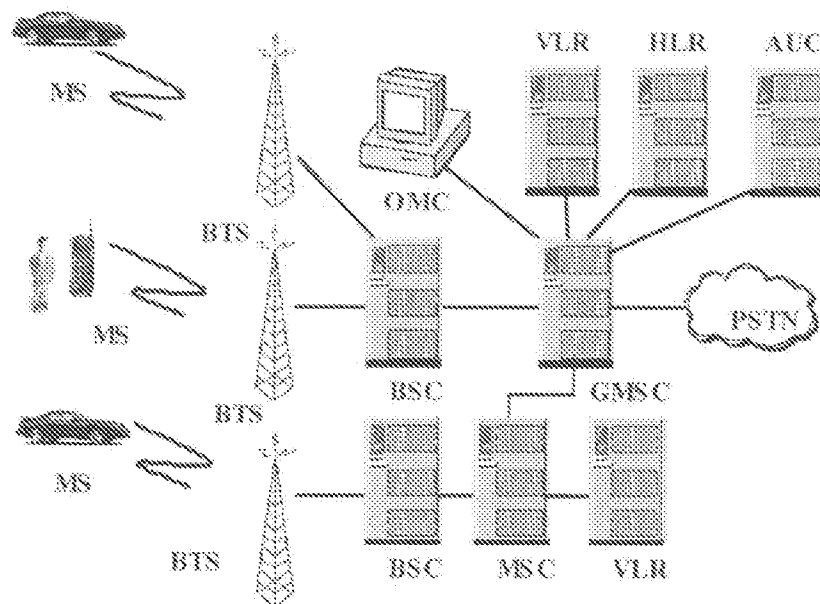


Fig. 6.1 An example of the wireless communication systems

By having the wireless communication systems in place, various mobile services have been provided to the mobile users, such as mobile voice and data services. The mobile data services include messaging services and wireless web services. The examples of the mobile messaging services are messaging through short message service (SMS), cell broadcast service (CBS), and unstructured supplementary services data (USSD). The examples of wireless web services include mobile commerce and mobile payment services.

### 6.3 Wireless Computing Infrastructure

The evolution of computing infrastructure has gone from the client-server infrastructure model, to the network computing infrastructure model. It is now moving toward the wireless computing infrastructure model. In the client-server computing infrastructure model shown in Fig. 6.2, many clients connect to a server. The server is a center of computing, to provide a variety of services that clients request. The client machines were equipped with dedicated client software. This model was very effective before the Internet was adopted.

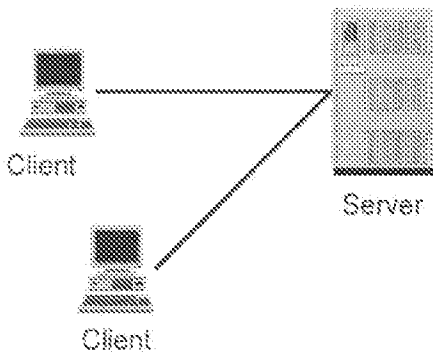


Fig. 6.2 Client-server computing infrastructure model

The Internet has changed the computing infrastructure. In the 1990s, many leading players in the computing industry looked into network computing. In the network computing infrastructure model shown in Fig. 6.3, the clients connect to the Internet, and the Internet connects a variety of servers. The client machines do not need special client software. Only standard Internet browser such as Netscape or Microsoft Internet Explorer is needed. This saves a huge effort for companies to

develop different client software. Through the Internet, clients can access much wider applications than they used to. The network computing infrastructure model coupled with the revolutionized Internet, has indeed changed the computing industry, corporate IT infrastructure, and people's daily lives.

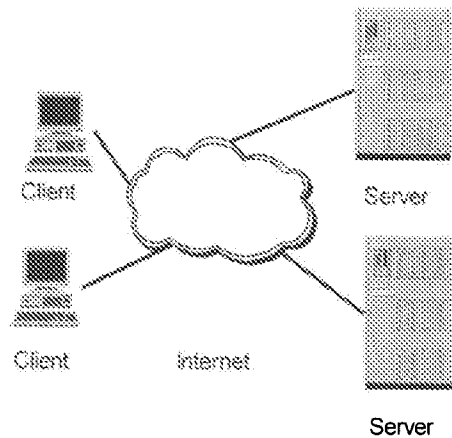


Fig. 6.3 Network computing infrastructure model

In the late 1990s, wireless communication was rapidly developed. Cellular phones and a variety of other wireless devices have become popular. The wireless communication infrastructure together with Internet technology makes another evolution step possible, resulting in the wireless computing infrastructure model shown in Fig. 6.4.

In addition to wireless communication infrastructure, the wireless computing-infrastructure model includes flexible and mobile devices, such as personal digital assistants (PDAs), mobile phones, pagers, hand-held organizers, and home-entertainment systems. These wireless devices connect to the Internet and provide quick access to many wireless applications. With enhanced security, electronic commerce transactions can also be conducted through these wireless devices. The differences between the network computing infrastructure model and the wireless computing infrastructure model are:

- In the wireless-computing-infrastructure model, client machines are no longer only the desktop PCs or laptop computers as those in the network computing infrastructure model. They can be any hand-held device with wireless communication capability.

- In the wireless-computing-infrastructure model, communication between clients and servers are no longer through wired lines as the case of the network computing infrastructure model. The communication is carried out through a wireless network and the Internet.
- In the wireless-computing-infrastructure model, there are two sets of communication protocols, one set is wireless protocols and the other set is the wired Internet protocols. This is different from the network computing infrastructure model in which, there is only wired Internet protocols.

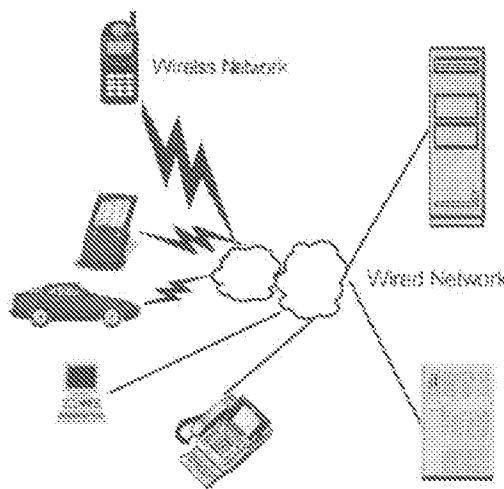


Fig. 6.4 Wireless computing infrastructure model

The challenges for the wireless-computing-infrastructure model include powerful wireless e-commerce applications for massive wireless users that are still to be developed and deployed, wireless-device capability-management systems, and personalization for different users, and the associated user management by the wireless service providers. Given the limitations that wireless devices have, the server software must be highly scalable and flexible. Mobility will also make the wireless applications be more interesting and challenging.

In the wireless-computing-infrastructure model, to make mobile commerce transactions successful, there are three very important principles: security, connectivity, and simplicity. The importance of the security model is obvious, as without the proper security protection of the consumer's financial account information and other private information, mobile commerce is not going to succeed. The connectivity loss during the mobile-commerce transaction will create the trustworthiness

problem on mobile commerce for consumers. People will not accept that their mobile-commerce transactions (such as mobile payments) are aborted due to a broken connection. Given a limited capacity of a mobile device and the reliability of the wireless connection compared to that of the wired connection, it is easy to see that simplicity and reliability are important for completing a mobile-commerce transaction instantly.

## 6.4 Wireless Application Protocol

### 6.4.1 WAP Overview

The wireless application protocol (WAP) is a suite of emerging standards to enable mobile Internet applications. The WAP standards have been created as a result of the WAP Forum that was formed in June 1997 by Ericsson, Motorola, and Nokia. The WAP Forum is designed to assist the convergence of two fast-growing network technologies, namely, wireless communications and the Internet. The convergence is based on rapidly increasing numbers of mobile-phone users and the dramatic affect of e-business over the Internet. The combination of these two technologies will have a big impact on current e-business practice, and it will create huge market potential.

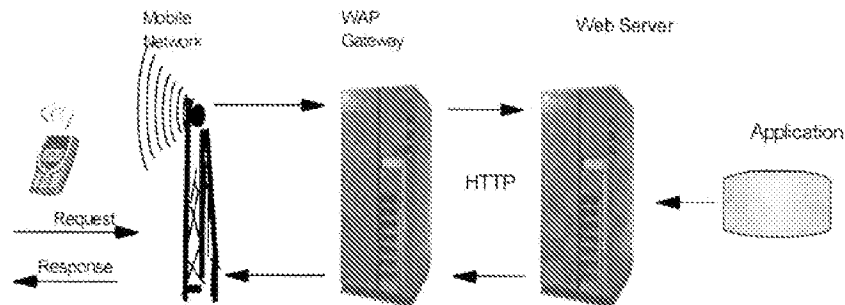


Fig. 6.5 The WAP architecture

The WAP standards consist of a variety of architecture components, including an application environment, scripting and markup languages, network protocols, and security features. These components and features together define how wireless data handsets communicate over the wireless network and how content and ser-



vices are delivered. With the WAP standards, a wireless data handset can establish a connection to a WAP compliant wireless infrastructure, request and receive the content and services, and present the content and services to the end user. This WAP-compliant wireless infrastructure may include the handset, the server side infrastructure, such as the proxy server (WAP gateway), the web server, the application server, and the network operator (telecommunication company). The WAP architecture is shown in Fig. 6.5.

The WAP architecture can also be presented through the WAP protocol stack shown in Fig. 6.6. The WAP protocol stack covers the complete picture from bearers to applications. The bearers are the various wireless networks that WAP currently supports. The transport layer is an interface common to the underlying wireless network, and it provides a constant service to the upper layers in the WAP stack, such that the bearer services are transparent to the upper layers. In other words, with the transport layer, the specific network characteristics can be masked. The security layer provides security for the transport layer, based on the industry standard protocol, the transport layer security (TLS) protocol. The transaction layer provides a lightweight transaction-oriented protocol for mobile thin clients. The session layer provides the application layer with the capability to select connection-oriented or connectionless services. The application layer deals with a general-purpose environment for applications.

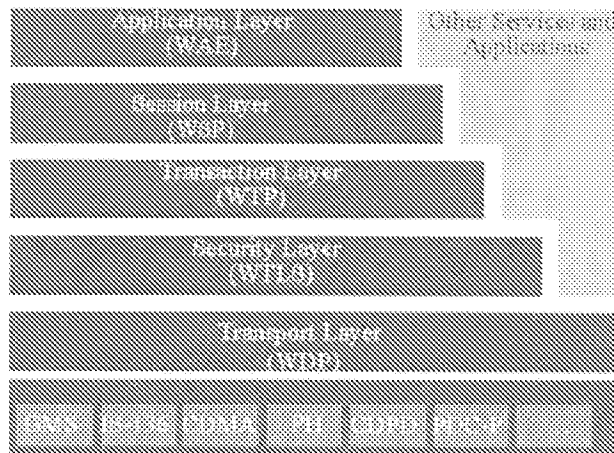


Fig. 6.6 The WAP protocol stack

The WAP protocols in Fig. 6.6 include wireless application environment (WAE), wireless session protocol (WSP), wireless transaction protocol (WTP), wireless transport layer security (WTLS), and wireless datagram protocol (WDP).

In the following sections, we discuss these protocols with a focus on WAE by providing more detailed information.

#### 6.4.2 Wireless Application Environment

The wireless application environment (WAE) consists of a set of standards that collectively define a group of formats for wireless applications and downloadable content. WAE specifies an application framework for wireless devices, such as cellular phones, pagers, and PDAs. WAE has two logical layers, namely, user-agent layer and format-and-service layer. The components of the user-agent layer include browsers, phone books, message editors, and other items on the user device side, such as wireless telephony application (WTA) agent. The components of the format-and-service layer include common elements and formats accessible to the user agents, such as WML, WMLScript, and WAP binary XML content format (WBXML).

A WAP microbrowser has the following capabilities:

- Submission requests to the server
- Reception of responses from the server
- Converting and parsing the data
- Interpreters from WML and WMLScript files
- Ability to interact with the appropriate WAP layer
- Local cache and variable management
- Wireless session protocol processing
- Effective management of local hardware resources, such as RAM, ROM, small screen, and input and output

#### Wireless Markup Language

Wireless markup language (WML) is a language based on the extensible markup language (XML). WML is optimized for small screens and limited memory capacity, and it is for content intended for lightweight, wireless devices such as mobile phones and personal digital assistants (PDAs).

A WML document is called deck. A page of a WML document is called card. A deck consists of one or more cards. Each deck is identified by an individual URL address, similar to an HTML page. A WML deck requires a browser that will format the deck for the benefit of the user. The browser determines the final shape of the deck. Sometimes, people use the analogy of HTML to explain WML. In the analogy, a WML deck corresponds to an HTML page. However, there are differences between a WML deck and an HTML page. While each HTML file is a single viewable page, a WML deck may contain multiple cards, each of which is a

separate viewable entity. WML files are stored as static text files on a server. During the transmission from the server to the browser, the WML files are encoded in binary format by the wireless connection gateway, and then sent to the browser. This is also different from HTML, where there is no need for such an encoding process.

WML contains commands for navigating in decks. Each WML command has two core attributes, namely, id and class. The id is the attribute for an individual name to the elements inside a deck, while the class is the attribute that links the element to one or several groups. A WML deck, at its most basic level, is constructed from a set of elements. Elements are identified by tags, which are enclosed in angle brackets. Each element must include a start tag (<el\_tag>) and an end tag (</el\_tag>). The content is included between the start and end tags. An empty element that has no content can be abbreviated by a single tag (<el\_tag/>).

Because WML is based on the XML language, a WML document must follow the XML rule to contain the XML specified document type definition (DTD) at the beginning of the WML code, which is referred to as deck header or document prolog, as follows:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
http://www.wapforum.org/DTD/wml\_1.1.xml>
```

A deck is defined by the <wml> and </wml> tags that are required in every WML document. Within a deck, each card is defined by the <card> and </card> tags. Both <wml>...</wml> and <card>...</card> are formatting commands. The <wml>...</wml> commands summarize the deck. The <card>...</card> commands summarize the text, images, input fields, and any other objects of a card in the deck.

Cards are the basic units of WML, defining an interaction between mobile device and the user. Each card may contain three different groups of elements: content elements (such as text, tables, and images), tasks and events (such as <on-event>, <timer>, and <do>), and data entry (such as <input> and <select>).

### WMLScript

WMLScript is a simple scripting language based on ECMAScript (ECMA-262 standard) with modifications to better support low-bandwidth communication and thin clients. WMLScript is part of the WAP application layer.

WMLScript complements the WML by adding simple formatting capabilities to make the user interfaces more readable, for example, the capabilities of checking the validity of user input and generating messages and dialog locally to reduce the

need for expensive round-trip to show alerts. These capabilities are not supported by WML as the content of WML is static. WMLScript provides programmable functionality that can be used over narrowband communication links in clients with limited capabilities. With WMLScript, more advanced user interface functions can be supported and intelligence can be added to the client. WMLScript also provides access to the device and its peripheral functionality and reduces the amount of bandwidth that is needed for sending data back forth between the server and the client.

WMLScript is similar to JavaScript. For example, WMLScript includes a number of operators such as assignment and arithmetic operators, which are similar to those in JavaScript. However, there are major differences between WMLScript and JavaScript. First, WML contains references to the URL address of a WMLScript function, whereas JavaScript functions are normally embedded in the HTML code. Second, WMLScript must be compiled into binary WMLScript code prior to its execution in a WAP device, while there is no such requirement for JavaScript.

Although WMLScript is based on ECMAScript as we mentioned before, there are differences between WMLScript and ECMAScript. First, like JavaScript, ECMAScript is not encoded in a binary form while WMLScript has to be. Second, to form WMLScript, many advanced features of the ECMAScript language have been dropped to make WMLScript smaller, and easier to compile into binary WMLScript code.

WMLScript syntactically resembles C language. It has basic types, variables, expressions, and statements. Unlike C, WMLScript cannot be used to write stand-alone applications. There is no built-in support for reading and writing files. Because it is an interpreted language, scripts or functions can run only in the presence of an interpreter, which is supplied as part of the WAP user agent. WMLScript is a weakly typed and object-based language, in which variables must be declared before they can be used in expression. In WMLScript, there is no main program or routine. Functions are created to perform specific tasks and they are invoked through a WML call. When a WMLScript function is invoked, the WAP gateway accesses the source code, compiles it into binary WMLScript code, and then sends the execution function to the WAP user agent. WMLScript code is written in normal text files with the file extension "wmls."

Each WMLScript file contains at least one function. Each function is composed of statements that perform the appropriate processing. The structure of a WMLScript function is as follows:

```
extern function function_xyz (parameter list)
{ // start of the statements
  statement_1;
  statement_2;
```

```

    statement_n;
  } // end of the statements

```

With this structure and the file extension “xmls,” a simple WMLScript example to set a first day of the week, which is included in the file named “setday.xmls,” is listed as follows:

```

extern function SetDay(givenDay)
{
    if (givenDay > 0 && givenDay <= 7) {
        var newDay = givenDay;
    }
    else {
        newDay = 1;
    }
    return newDay;
}

```

To invoke a WMLScript function, a reference to the WMLScript function must be included in a WML document. The call will be routed from the WAP browser through the WAP gateway to the server. The server then sends the binary WMLScript code to the WAP browser. The WAP browser has an interpreter that is able to execute WMLScript programs in their binary format. Using our example, the reference to the WMLScript can be as simple as follows:

```

<do type="ACCEPT" label="Set Day">
<!--Calling the WMLScript function: -->
    <go href="setday.xmls#SetDay($(givenDay))"/>
</do>

```

### **Wireless Telephony Application Interface and Wireless Telephony Applications**

One of the major mobile services is voice. How can we set up a call or receive an incoming call using a WAP enabled mobile device? This is the problem that Wireless Telephony Application Interface (WTAI) addresses. WTAI is designed to allow wireless network operators access the telephony features of WAP device. Through either a WML deck/card or WMLScript, using the WTAI function libraries, a mobile phone call can be set up and an incoming call can be received. In addition, text messages can be sent or received, and phonebook entries can be manipulated on the WAP device.

Wireless telephony applications (WTA) is a collection of telephony-specific extensions for call and feature control mechanisms that make advanced mobile net-

work services available to the mobile users. It provides a bridge between wireless telephony and data. The WTA applications can use the privileged WTAI.

From the architecture point of view, a WTA server communicates with the WAP gateway to deliver and manage telephony services; on the client side, there is a WTA framework which has three components as follows:

1. User agent: This agent supports the WTAI libraries, renders WML, and executes WMLScripts.
2. Repository: It provides persistent client-side storage for wireless telephony applications.
3. Event Handling: This deals with incoming-call and call-connected events to be delivered to a wireless telephony application for processing, which may also invoke WMLScript library interfaces to initiate and control telephony operations.

Wireless telephony supports in WAP make WAP suitable for creating mobile applications through voice services. The compact form, encryption, and error handling capabilities of WAP enable critical wireless payment transactions.

## **WBXML**

WAP Binary XML Content Format (WBXML) is defined in the Binary XML Content Format Specification in the WAP standard set. This format is a compact binary representation of the XML. The main purpose is to reduce the transmission size of XML documents on narrowband communication channels.

A binary XML document is composed of a sequence of elements and each element may have zero or more attributes. The element structure of XML is preserved while the format encodes the parsed physical form of an XML document. This allows user agents to skip elements and data that are not understood. In terms of encoding, a tokenized structure is used to encode an XML document. The network byte order is big-endian, that is, the most significant byte is transmitted first. Within a byte, bit-order is also big-endian, namely, the most significant bit first.

### **6.4.3 Wireless Session Protocol**

The Wireless session protocol (WSP) is a protocol family in the WAP architecture, which provides the WAP Application Layer with a consistent interface for session services. WSP establishes a session between the client and the WAP gateway to provide content transfer: the client makes a request, and then the server answers with a reply through the WAP gateway. WSP supports the efficient operation of a WAP micro-browser running on the client device with limited capac-

ity and communicating over a low-bandwidth wireless network. The WSP browsing applications are based on the HTTP 1.1 standard, and incorporated with additional features that are not included in the HTTP protocol, for example, the connection to the server shall not be lost when a mobile user is moving, resulting in a change from one base station to another. The other additional features that WSP supports include:

- **Binary encoding:**  
Given the low bandwidth of the wireless network, the efficient binary encoding of the content to be transferred is necessary for mobile Internet applications.
- **Data push functionality:**  
Data push functionality is not supported in the HTTP protocol. A push is what is performed when a WSP server transfers the data to a mobile client without a preceding request from the client. WSP supports three push mechanisms for data transfer, namely, a confirmed data push within an existing session context, a non-confirmed data push within an existing session context, and a non-confirmed data push without an existing session context.
- **Capability negotiation:**  
Mobile clients and servers can negotiate various parameters for the session establishments, for example, maximum outstanding requests and protocol options.
- **Session suspend/resume:**  
It allows a mobile user to switch off and on the mobile device and to continue operation at the exact point where the device was switched off.

WSP offers two different services, namely, the connection-oriented service and the connectionless service. The connection-oriented service has the full capabilities of WSP. It operates on top of the wireless transaction protocol (WTP), supports session establishment, method invocation, push messages, suspend, resume and session termination. The connectionless service is suitable for these situations where high reliability is not required or the overhead of session establishment and release can be avoided. It supports only basic request-reply and push, and does not rely on WTP.

#### 6.4.4 Wireless Transaction Protocol

The wireless transaction protocol operates on top of a secure or insecure datagram service. WTP introduces the notion of a transaction that is defined as a request

with its response. This transaction model is well suited for web content requests and responses. It does not handle stream-based applications (such as telnet) well.

WTP is responsible for delivering the improved reliability over datagram service between the mobile device and the server by transmitting acknowledge messages to confirm the receipt of data and by retransmitting data that has not been acknowledged within a suitable timeout period.

WTP supports an abort function through a primitive error handling. If an error occurs, such as the connection being broken down, the transaction is aborted.

WTP is message-oriented and it provides three different types of transaction services, namely, unreliable one-way, reliable one-way, and reliable two-way transactions. The transaction type is set by the initiator and it is contained in the service request message sent to the responder. The unreliable one-way transactions are stateless and cannot be aborted. The responder does not acknowledge the message from the initiator. The reliable one-way transactions provide a reliable datagram service that enables the applications to provide reliable push service. The reliable two-way transactions provide the reliable request/response transaction services.

#### **6.4.5 Wireless Transport Layer Security**

The wireless transport layer security (WTLS) protocol is a security protocol based on the *transport layer security protocol* (TLS) [6.10] (see Section 6.7). TLS is a derivative of the *secure sockets layer* (SSL), a widely used security protocol for Internet applications and payment over the Internet (for more information about SSL, see Section 11.6 of Chapter 11). WTLS has been optimized for the wireless communication environment. It operates above the transport protocol layer.

WTLS is flexible due to its modular design. Depending on the required security level, it can be decided whether WTLS is used or not. WTLS provides data integrity, data confidentiality, authentication, and denial-of-service protection. The data integrity is to ensure that data sent between a mobile station and a wireless application server is unchanged and uncorrupted. The data confidentiality is to ensure that data transmitted between the mobile station and the wireless application server is private to the sender and the receiver, and it is not going to be understood by any hackers. The authentication is to check the identity of the mobile station and the wireless application server. The denial-of-service protection is to prevent the upper protocol layers from the denial-of-service attacks by detecting and rejecting data that is replayed or not successfully verified.



#### 6.4.6 Wireless Datagram Protocol

The wireless datagram protocol (WDP) in the WAP architecture specifies how different existing bearer services should be used to provide a consistent service to the upper layers. WDP is used to hide the differences between the underlying bearer networks. WDP layer operates above the bearer services and provides a consistent interface to the WTLS layer.

Different bearers have different characteristics. The bearer services include short message, circuit-switched data and packet data services. Since WAP is designed to operate over the bearer services, and since the bearers offer different types of quality of service with respect to throughput, error rate, and delays, the WDP is designed to adapt the transport layer to specific features of the underlying bearers. The adaptation results in a family of protocols in the WDP layer, dealing with each supported bearer network protocol. When a message is transmitted through WAP stack, depending on the underlying bearer network, a different WDP protocol may be used. For example, for an IP bearer, the user datagram protocol (UDP) must be adopted as the WDP protocol, and for a short message service (SMS) bearer, the use of the source and destination port numbers becomes mandatory.

#### 6.4.7 WAP Gateway

A WAP gateway as shown in Fig. 6.7 is a proxy server that sits between the mobile network and the Internet. The purpose of this proxy server is to translate between HTTP and WSP. The reason for the translation is that the web server connected to the Internet only understands the HTTP protocol while the WAP-enabled mobile client only understands the WSP. The WAP gateway also converts a HTML file into a WML document that is designed for small-screen devices. In addition, the WAP gateway compiles the WML page into binary WML which is more suitable for the mobile client. The WAP gateway is transparent to both the mobile client and the web server.

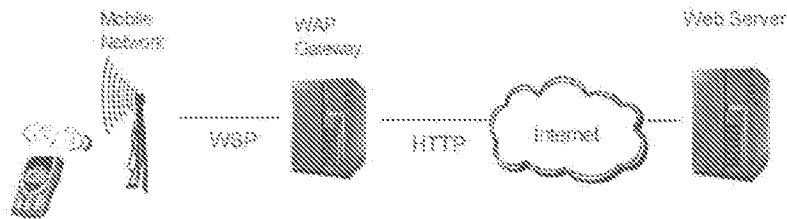


Fig. 6.7 WAP gateway

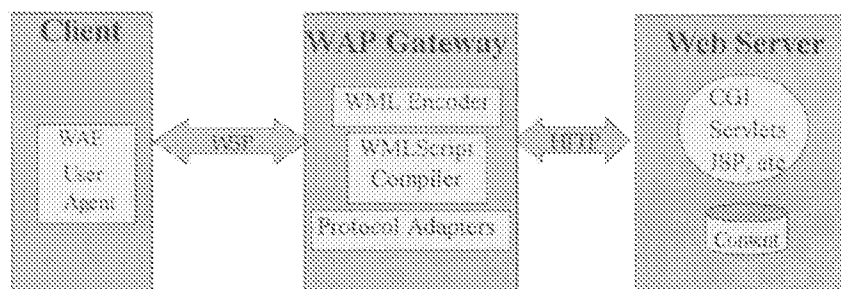


Fig. 6.8 WAP model

Fig. 6.8 shows the WAP model using the WAP gateway. How the WAP gateway processes a typical request for a document can be illustrated as follows:

1. The mobile user makes a request for a specific document using the WAP phone.
2. The WAE user agent on the WAP phone encodes the request and sends it to the WAP gateway.
3. The WAP gateway decodes and parses the encoded request.
4. The WAP gateway sends a HTTP request for the document.
5. The web server answers with a response to the WAP gateway.
6. The WAP gateway parses and encodes the response.
7. If the content-type is WML then the gateway compiles it into binary WML.
8. The WAP gateway sends the encoded response to the WAP phone.
9. The WAE user agent on the WAP phone interprets and presents the document to the mobile user.

## 6.5 Wireless Security

Wireless security is becoming more and more important as transaction-based mobile commerce applications (such as mobile payment, banking, and buying stock via cellular phones or handheld devices) take off.

The basic security needs for mobile commerce are similar to that for electronic commerce over the wired Internet, such as authentication, confidentiality, non-repudiation, and data integrity. However, implementing them in the wireless world

is more difficult than it is to implement them in the wired world. This is simply because the limitations that wireless have, including limited bandwidth, high latency, and unstable connections. In addition, limited battery power and limited processing power that the wireless devices have also make the sophisticated security algorithms difficult to run on these devices.

As we discussed in the previous section, WAP does specify an SSL like security protocol, namely, wireless transport layer security (WTLS). However, there are some drawbacks in WTLS. First, WTLS only provides security protection from the mobile client to the WAP gateway where the wireless communication ends. In the wired Internet environment, when a web client (web browser) starts an SSL session with web server, the web client and web server are communicated directly, and the end-to-end security protection is provided through the SSL session. This means when one sends a credit card number over SSL, only the receiving web server will be able to receive it. The situation is different in the WTLS. The credit card number will be securely protected between the mobile device and the WAP gateway. It will be in the clear form at the WAP gateway. Then, an SSL session will be established between the WAP gateway and the Web server for securely transmitting the credit card number over the Internet. This means that there is no end-to-end security protection for the wireless transactions since there is a potential security hole in the WAP gateway. Second, the CCITT X509 certificate is too large for the mobile phones, and the limitations of the processing power and battery for the wireless devices make it difficult to perform the sophisticated computation of the public-key encryption. In summary, WAP security has two issues: (1) there is no end-to-end security protection, and (2) there is a lack of certificates for mobile devices.

People are currently addressing these two security issues. As a result, simplified certificates have been defined for mobile devices. The research on how to use currently available mobile devices to perform the computation of public-key encryption is ongoing. For example, elliptic curve cryptography (ECC) requires far fewer resources and it looks very promising for wide deployment to CPU-starved wireless devices.

## 6.6 Summary

The convergence of wireless technologies and the e-commerce over the Internet lead to emerging and fast growth of mobile commerce. As the result, mobile commerce and mobile payment have attracted more and more attention of the academic researchers and business leaders. Being able to conduct e-commerce and make payment anywhere and anytime is becoming reality. However, because of the limitations that wireless have, conducting e-commerce and making payment in the wireless world is more difficult than in the wired world. Understanding the

wireless infrastructure that the wireless applications rely on is important for developing and deploying such applications.

In this chapter, we discussed the wireless infrastructure for mobile payment and fore mobile commerce in general, including wireless communication infrastructure, wireless computing infrastructure, wireless application protocol, and wireless security.

## 6.7 Appendix

### Overview of the Transport Layer Security

The transport layer security (TLS) [6.10] is a protocol that provides privacy and data integrity between two communicating applications. The TLS is application protocol independent, that is, higher-level protocols can layer on top of the TLS protocol transparently. The TLS protocol is composed of two layers:

- **TLS record protocol:** This protocol provides connection security and is used for encapsulation of various higher-level protocols, such as the TLS handshake protocol to be discussed below. It has the following two basic properties.
  - The connection is private. Data encryption is used for ensuring the communication privacy, and is based on symmetric cryptographic algorithms, such as DES or RC4. The keys for symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol (e.g., the TLS handshake protocol). The record protocol can also be used without encryption.
  - The connection is reliable. A message integrity check based on a keyed MAC is used for protecting message transport. Secure hash functions, such as SHA and MD5, are used for MAC computations. In the case of that another protocol uses the record protocol and negotiates security parameters, the record protocol can operate without a MAC.
- **TLS handshake protocol:** This protocol allows the server and client to authenticate each other, and negotiate an encryption algorithm and cryptographic keys. It has the following three basic properties.
  - The authentication between the server and client can be based on a public-key cryptographic algorithm, such as RSA or DSS. Although

the authentication can be mutual, the mutual authentication is optional. Generally speaking, one-way authentication is required.

- It is secure for the negotiation of a shared secret between the server and client.
- The negotiation is reliable.

Because the TLS is a derivative of SSL, the actual handshake exchanges are similar to that of SSL. The descriptions of the main SSL exchanges can be found in Section 11.6 of Chapter 11.

## 6.8 References

- [6.1] WAP. <http://www.ini.cmu.edu/netbil>.
- [6.2] Wireless Application Protocol Forum Ltd. (1999) Official wireless application protocol. Wiley, New York.
- [6.3] S. Mann, S. Sbihli (2000) The wireless application protocol. Wiley, New York.
- [6.4] S. Singhal, et al. (2001) The wireless application protocol. Addison-Wesley, New York.
- [6.5] J. Schiller (2000) Mobile communications. Addison-Wesley, New York.
- [6.6] U. Hansmann, et al. (2001) Pervasive computing handbook. Springer, Berlin Heidelberg New York.
- [6.7] C. Sharma (2001) Wireless Internet enterprise applications. Wiley, New York.
- [6.8] Y. B. Lin, I. Chlamtac (2001) Wireless and mobile network architectures. Wiley, New York.
- [6.9] A. Dornan (2001) The essential guide to wireless communications applications. Prentice-Hall, New York.
- [6.10] T. Dierks, C. Allen (1999) The TLS protocol version 1.0. <http://www.ietf.org/rfc/rfc2246.txt>.

## **7 Payment Agents**

Amitabha Das

School of Computer Engineering  
Nanyang Technological University, Singapore

### **7.1 Introduction**

In a broad sense, a software agent is a computer program that acts autonomously on behalf of a person or organization. Software-agent technology seems able to provide attractive solutions in the field of electronic commerce. An agent-based architecture for electronic commerce allows the creation of a virtual marketplace in which a number of autonomous or semi-autonomous agents trade goods and services. The introduction of software agents acting on behalf of end-consumers could reduce the effort required from users when conducting electronic commerce transactions, by automating a variety of activities. The personalized, continuously running autonomous nature of agents makes them well suited for mediating consumer behavior with respect to information filtering and retrieval, personalized evaluations, complex coordination, and time-based interactions. Agents are able to examine a large number of products before making a decision to buy or sell. This not only eliminates the need to manually collect information about products but also allows the negotiation of an optimal deal with the various sellers of a good.

#### **7.1.1 Agent-Based Electronic Commerce Systems**

During the hay day of the dotcoms, several agent-based e-commerce systems came into existence, e.g., PersonaLogic, Firefly, BargainFinder, and Jango. All of them disappeared within a short while. PersonaLogic allowed users to specify product features and used a constraint satisfaction algorithm to filter through the product space to retrieve an ordered set of products. Firefly used an automated collaborative filtering method to rate and recommend products to shoppers. BargainFinder and Jango were systems that could take a product name as the input, obtain price information from other websites, and perform a price comparison.

More advanced systems in which buyer and seller agents cooperate to constitute a virtual market have also been developed in academic institutions (e.g., [7.1-7.6]). Among them Kasbah [7.1] is a multi-agent system where agents filter through ads on behalf of their owners and find those that their users might be interested in. The agents then proceed to negotiate to buy and sell items. MAGMA [7.6] is a prototype of a virtual marketplace system, which consists of multiple trader agents, an advertising server, and a bank. Trader agents are responsible for buying and selling goods. They also handle the price negotiations. Advertising server provides a classified advertisement service that includes search and retrieval of ads by category. Bank provides a set of basic banking services that includes checking accounts, lines of credit, and electronic cash.

### 7.1.2 Use of Agents for Payment

In none of the agent-based e-commerce systems discussed above are the agents used for executing the actual transaction involving transfer of money. Besides, in all the above systems, the agents are immobile. They do not support mobile users, and for activities that require a large number of interactions between remote agents they leave much to be optimized.

However, when the system is based only on static agents that reside in sites controlled entirely by their owners, there is no real reason for not allowing the agents to execute the payment operations. The security concerns in this case are not different from those when the payment involves manual intervention by the transacting parties. In spite of that, so far, the introduction of a system in which the agents carry out autonomously the entire process of e-commerce transaction starting from information gathering to the completion of the transaction has not materialized. The real reason for this is perhaps the lack of confidence in the competence of the agents to take decisions that are intelligent enough.

The security concerns, however, change drastically when it comes to the introduction of *mobile agents*. A mobile agent is a program that represents a user and can migrate autonomously from node to node in a computer network to perform some computation on behalf of the user. It is not bound to the system where it begins execution. It can suspend its execution at an arbitrary point, transport itself to another node, and resume execution there.

The mobile-agent paradigm offers several advantages compared to traditional approaches, such as a reduction in communication costs, better support of asynchronous interactions, enhanced flexibility in the process of software distribution, and the offer of increased performance and robustness. The use of mobile agents has been particularly promising in the fields of information retrieval, network management, electronic commerce, and mobile computing.

Information-retrieval applications often download and process large amounts of information from the server over the network while generating a comparatively small amount of result data. This can be supported much more efficiently if a mobile agent representing a query moves to the server where the data are actually stored, rather than having to move all of the data across the network for filtering. Then vendors can set up online shops with products or services for sale. Mobile agents can help customers locate the best offerings, can negotiate deals, and can even conclude transactions on behalf of their owners.

Finally, an important application of mobile agents concerns mobile computing. A portable computer's network connectivity is often achieved through low-bandwidth wireless links, hence it is likely to be slow. Besides, to minimize power consumption and transmission costs, users will not want to remain online while some complicated query is handled on their behalf by the fixed computing resources. Mobile agents offer a promising way of achieving this: users simply submit mobile agents that embody their queries and log off, waiting for the agents to deposit their results, ready to be picked up at a later time.

## **7.2 Security Implications of Mobile-Agent-Based Systems**

The fact that mobile agents can and do execute in hosts other than the ones controlled by their owners gives rise to a number of security concerns that do not exist in the case of static agents. The most important and the most difficult-to-handle security threat arises from the fact that the third-party host has complete access and observability of the code of the mobile agents. As a result, it is extremely easy for a malicious host to either spy on confidential information, or tamper with the execution of the mobile agents.

This appears to be a severe limitation on the applicability of mobile agents in tasks involving confidentiality or security, such as electronic payment operation. However, a number of possible remedies have been suggested to overcome this problem. We will briefly examine these before we embark on the task of designing a secure payment protocol for mobile agents in untrusted host environments.

## **7.3 Security Techniques Protecting Mobile Agents**

Methods that protect an agent against attacks can be categorized into those that prevent attacks and those which detect attacks. The detection methods use cryptographic and other techniques to detect tampering with the code and/or data carried



by the mobile agent. The detection techniques are useless in preventing an attack, such as the theft of confidential information, and only serve to help in post mortem analysis. In the context of payment protocols, such methods can come in handy in detecting whether the payment has been redirected maliciously to an unintended recipient.

On the other hand, the prevention techniques are more relevant in thwarting attacks. Some of the prevention techniques proposed in the literature are *sliding encryption* [7.7], trail obscuring, code obfuscation [7.8], and computing with an encrypted function [7.9-7.10]. These are briefly discussed below.

### 7.3.1 Methods for Protecting Mobile Agents

#### Sliding Encryption

A mobile agent uses this technique [7.7] to encrypt acquired data by using a public key. The key is public, so theft is not an issue. Decryption can only be performed with the corresponding private key. The mobile agent uses sliding encryption to hide what it is carrying, so potentially malicious hosts that the mobile agent visits cannot steal any data.

This technique is applicable when mobile agents gather information in small chunks from multiple sources and it is necessary to prevent any host other than the source of a given piece of information from seeing it. As an example, consider a scenario where a mobile agent is collecting product information from multiple vendor sites and accumulating the information in its buffer. When it visits a host, the host can potentially see all the information the mobile agent is carrying and can possibly tamper with it for its own commercial gain or to affect the operations of the predecessor nodes.

A straightforward use of public key cryptography can result in substantial storage overhead for an agent. As an example, suppose that the agent is required to collect 4 bytes of data from each of 1024 different sites. If it uses a 128-byte public key, then it must encrypt the 4 bytes of data collected from a node into at least a 128-byte ciphertext before it moves on to a subsequent node. Consequently, in the end, the agent must have the capacity to carry 128 Kbytes of ciphertext which contains only 4 Kbytes worth of plaintext.

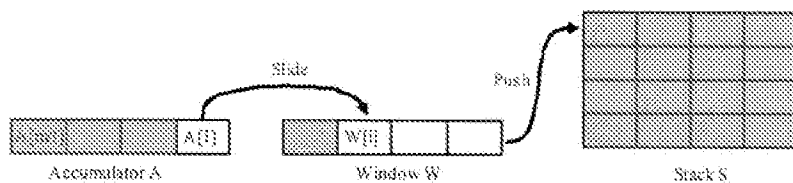


Fig. 7.1 Data structures used for sliding encryption

The technique of sliding encryption [7.7] helps to reduce the size of the ciphertext substantially by using the method of chain ciphering (see Fig. 7.1). The scheme described is based on the RSA [7.11] public-key encryption algorithm, but it is general enough to accommodate any other public-key encryption algorithm. The essentials of the scheme are described below.

Assume that the granule of plaintext that is collected from each site is of a small fixed length  $u$ . This is concatenated with randomly generated  $v$  bytes to construct a word of size  $v+u$  in which the random word occupies the upper-order bytes. Let us call this composite word  $X$  which is of length  $t = u+v$ . The length of the RSA public key used is  $m$ . Both  $m$  and  $t$  are powers of 2, and  $m \gg t$ .

The data structures used by the agent for sliding encryption include an accumulator  $A$  of  $m$  bytes, an  $m$ -byte window  $W$ , and a stack  $S$ , each stack element  $S[i]$  being  $m$  bytes long. The accumulator is divided into  $m/t$  entities, each  $t$  bytes long.  $A[1]$  contains the least-significant bytes of  $A$ , and  $A[m/t]$  contains the most-significant bytes. We will denote the public-key encryption function by  $E()$  and the corresponding private-key decryption by  $D()$ . The functions  $E()$  and  $D()$  include an uneven Feistel-like preprocessing and postprocessing as in [7.12].

The mechanism works as follows. Initially the stack is empty, and the accumulator is initialized to a random non-zero positive integer  $K$ . After the piece of information is collected at the first site, the composite word  $X_1$  is formed by concatenating it with the randomly generated  $v$  bytes. Then  $A[1]$  is replaced by  $X_1$ , and the resultant content of the whole accumulator is encrypted using  $E()$ .  $A[1]$  now contains the lowest-order bytes of the ciphertext. Then we set  $W[m/t] = A[1]$ . The remaining part of the ciphertext in the accumulator is carried unchanged and serves as a link in the chain ciphering process.

In the next node, the composite word  $X_2$  is similarly formed from the information picked up at that node, then  $A[1]$  is replaced by  $X_2$ . The modified content of the accumulator is now encrypted using  $E()$ , and again the lowest bytes of the ciphertext, which now occupy  $A[1]$ , slide into  $W[(m/t)-1]$ .

After all the  $m/t$  slots in the window  $W$  are full, it is pushed onto the stack  $S$ , and the sliding restarts from slot  $W[m/t]$ .

After all the nodes are visited and the mobile agent returns to its owner, the decryption process starts. This makes use of the private key and the process simply reverses the encryption steps sequentially, retrieving the hidden pieces of information in reverse order.

### **Trail Obscuring**

This method depends on changing a mobile agent binary image to make it hard to identify by pattern matching. A mobile agent attempts to obscure its path through the network by constantly modifying its own binary image so that it cannot be identified as the same mobile agent by different hosts which are colluding in an attempt to track the mobile agent. This works in a situation where anonymity is required, such as an anonymous monetary donation or auction bid. It may also aid in surviving malicious hosts trying to stop specific behavior that can be identified by analyzing the mobile agent's path.

One important component of traceability of a mobile agent is its state information. If a group of adversary nodes compare the state information of a mobile agent captured in the snapshots taken by them, it can be possible to determine the order in which the nodes were traversed. Therefore, to thwart such attacks, the state information associated with an agent must be concealed. As an example, if sliding encryption is used as described above, then the state information will consist of the accumulator values, the window values, the stack, the stack pointer, and the index to the next location in the window where the next value of  $A[1]$  will slide into. In this case, one has to devise ways to conceal the real state using various techniques. For details the reader is referred to [7.7].

However, trail obscuring is not a foolproof method. A major problem of this approach is that mobile agents cannot encrypt and decrypt themselves, because, if they could, then any host could also do the same as it too will have access to the decryption key. Suppose that a subset of all the nodes visited by the mobile agent colludes to trace the agent's itinerary by taking snapshots of the agent while it was visiting each node of this subset. Under such circumstances, it is impossible to make an agent completely untraceable if all the adversaries are connected directly, and the agent cannot modify itself without being caught just before moving out of an adversary node.

### **Code Obfuscation**

This method was discussed in [7.8]. Most of the above security problems can be solved if the host is not able to determine the relation between single lines of code

and their semantics and the relation between memory bits and the semantics of data elements, respectively. A host can of course modify code, data and control flow anyway, but not with a computed effect. For a host this results in three choices:

- Host can execute the agent undisturbed.
- Host can execute the agent by switching some bits, not knowing about the effect on the execution.
- Host can take the agent without executing it.

An attacker needs a certain amount of time to read the data, understand the code and, thereafter, manipulate both in a meaningful way. The basic idea of the approach described now is simply not to give them enough time to do this. According to [7.8] this can be achieved by a combination of code mess-up and a limited lifetime of code and data.

With the employment of code mess-up techniques, Hohl has developed a non-cryptographic agent protection scheme that is built up like any cryptographic mechanism: readable input (i.e., code and data) is transformed to an unreadable form by a mechanism that cannot be inverted easily with the current knowledge.

Code mess-up does cost something, both in terms of speed and of space, and the processing model is more complex due to expiration aspects. Therefore, this scheme should be mainly used for agents that need to be protected, e.g., because they carry money or other sensitive data. The global usage of this mechanism even for nonsensitive applications may be too expensive, but because a code mess-up infrastructure is needed only for protected agents, agents of both protection levels can exist and interact in parallel. Hohl claims that it is possible to practically protect agents from malicious hosts by using code mess-up techniques. However, future work has to prove this claim.

### Computing with Encrypted Function (CEF)

This method of concealing the computations of an agent from its host is proposed in [7.9] and [7.10]. Instead of using the more general term *program*, the authors differentiate between a function and the program that implements it. Thus, the goal is to encrypt functions such that their transformation can again be implemented as programs. The resulting program will consist of cleartext instructions that a processor or interpreter understands. What the processor will not be able to understand is the “program’s function.” With the requirements of mobile agents in mind, we can state the problem that we want to solve, as follows.

Alice has an algorithm to compute a function  $f$ . Bob has an input  $x$  and is willing to compute  $f(x)$  for her, but Alice wants Bob to learn nothing sub-

stantial about  $f(\cdot)$ . Moreover, Bob should not need to interact with Alice during the computation of  $f(x)$ . To let Alice and Bob work together in the way described above, we assume that a function  $f$  can be transformed (encrypted) to some other function  $E(f)$ . The encryption hides the function  $f$  and may or may not also contain the encryption of the output data. We let the notation  $P(f)$  stand for the program that implements the function  $f$ . In this protocol Alice does not send to Bob the program  $P(f)$  for the plain function  $f$  but the program  $P(E(f))$  for the encrypted function  $E(f)$ . Bob only learns about the program  $P(E(f))$  that he has to apply to his input  $x$  and the result of this computation that he has to return to Alice. The simple protocol for noninteractive computing with encrypted functions looks like this:

- (1) Alice encrypts  $f(x)$ .
- (2) Alice creates a program  $P(E(f))$  which implements  $E(f)$ .
- (3) Alice sends  $P(E(f))$  to Bob.
- (4) Bob executes  $P(E(f))$  on  $x$ .
- (5) Bob sends  $P(E(f))(x)$  to Alice.
- (6) Alice decrypts  $P(E(f))(x)$  and obtains  $f(x)$ .

Noninteractive computing with encrypted functions is a challenge for cryptography. The challenge is to find encryption schemes for arbitrary functions. The authors of [7.9] identified some specific function classes (i.e., polynomials and rational functions) for which they could find encrypting transformations.

Their approach of studying algebraic homomorphic encryption schemes (HES) yields a first and simple scheme for CEF. However, they leave it open whether the CEF approach is applicable to arbitrary functions, that is, they don't even claim to have achieved a complete solution for the case of all polynomials. However, within the restricted setting of polynomials and rational functions they can prove first positive results that falsify the "general belief on mobile code vulnerability" for nontrivial cases.

#### **7.4 Secure Payment Protocols Using Mobile Agents in an Untrusted Host Environment**

With the above background we are now in a position to explore ways to design payment protocols for mobile agents that offer security against malicious hosts. In order to do that we need to define precisely the context in which the mobile agents

operate and the specific threats of attacks they face. The following two sections define these parameters.

#### **7.4.1 Model for the Mobile-Agent-Based E-Commerce Environment**

There are mainly four parties in the payment system [7.13-7.14]: a bank B, a customer U, a merchant M, and a *trusted third party* (TTP). A TTP is an impartial entity that is trusted by both the customer and the merchant and whose testimony is accepted in a court of law as valid evidence. In addition, we assume the existence of a trusted certification authority that can certify the validity of the public keys of the different parties. Both customer U and Merchant M have accounts with the bank B. An electronic payment system consists of protocols that allow customer U to make a payment to the merchant M. The customer's site can create some buyer agents to do the information gathering, negotiation, and payment for him. The merchant's site can create some seller agents to interact with the customer or buyer agent. The bank can create one or more bank agents that can interact with the buyer agent and seller agent, providing some services, such as creating accounts, withdrawing and depositing money, transferring money, etc. TTP is used to provide a non-repudiation service in case any party should deny sending or receiving information in the protocol.

The buyer agents for the customer are hosted by a network of mobile agent hosts (MA hosts). These hosts provide a resident and executive environment for all these buyer agents.

In order to make the payment, the mobile agents have to communicate and transfer messages to one another. So the system must provide a mechanism for finding the current location of an agent and the MA host. All the entities, such as the customer U, Merchant M, Bank B, TTP, and all the MA hosts are assigned unique names. So that an agent can specify its desired destination when it migrates, a name server is provided which maps a symbolic name to the current location of the named entity. The locations of the customer, merchant, Bank, TTP, and MA hosts do not change often, whereas the location of a mobile agent is more likely to change. Whenever a mobile agent arrives or migrates to a new host, it should contact and inform the name server regarding its change of address, so that it can be located afterwards.

#### **Threat Model**

In this model, one or more agents representing a customer need to transfer sensitive payment information to the merchant site. The customer agents are hosted by a network of MA hosts. Both the MA hosts and the merchant site can be mali-

cious. The following is a list of assumptions regarding the nature of the potential attacks in the scenario described above:

- A1. At the most *m-1* malicious hosts may collude to steal sensitive information from the customer agent.
- A2. The mobile agents travel through secure channels, i.e., no one other than the intended recipient can gain any information by eavesdropping on the communication channels.
- A3. The merchant may deny that he has received the electronic money, and spend the money as his own later.
- A4. The merchant site host works independently and does not collude with malicious MA hosts to cheat the customer.
- A5. There is a “trusted third party” which is honest, and both the customer and the merchant trust that the TTP will execute its role correctly. The TTP has no role to play in the protection of the customer agents against malicious MA hosts.

#### 7.4.2 A Secure Payment Protocol

Since electronic payment necessarily involves processing and transfer of confidential information, mobile payment agents are extremely vulnerable to attacks by malicious hosts. The CEF technique described above can be an effective tool to protect mobile agents from malicious hosts, but its applicability is quite restricted because of the limited current knowledge of the functions. An alternative is to ensure that at no point in time is the confidential information completely accessible to the untrusted hosts. This approach is adopted in the following protocol by making use of secret sharing schemes. The basic protocol described below [7.13-7.14] is based on Shamir’s secret sharing scheme [7.15] and can use any digital cash scheme such as Chaum’s digital cash [7.16] or the more efficient e-cash scheme of Stefan Brands [7.17-7.18]. But it can be adapted to many other payment methods and can be based on other secret sharing techniques as well.

#### 7.4.3 Main Phases of the Protocol

There are four phases in the payment protocol:

1. **Withdrawal phase:** In this phase the customer withdraws electronic cash from their bank. The specifics of this phase will depend on the e-cash

scheme being adopted, and the subsequent phases are largely independent of this phase. At a conceptual level, it suffices to view this phase as generating some tokens which we call e-cash.

2. **Distribution phase:** In this phase, the customer encrypts the e-cash using a secret key and divides the secret key into several small shares using an  $(m, n)$  threshold scheme.
3. **Payment phase:** In this phase,  $m$  mobile agents work together and each passes its share of the secret key to the merchant's site. The merchant then reconstructs the secret key and deciphers the e-cash. Payment by e-cash typically involves a token transfer phase followed by an authentication phase in which the payee poses a challenge and the payer responds with appropriate values. The authentication phase can be handled by a single agent. For the sake of simplicity, we will confine our attention to the phase involving the transfer of the token only.
4. **Verification and transfer phase:** The merchant signs the e-cash deciphered in the payment phase and forwards it to bank B. The bank verifies that the e-cash submitted is not fake or duplicated and credits the amount to the merchant's account.

The core Secure Payment protocol consists of the Distribution Phase and the Payment Phase. In what follows we describe these phases in detail. But before we do so, the notation used is explained.

**Notation:**

- $M$ : The merchant (or payee).
- $s$ : Secret key for encrypting e-cash.
- $C$ : The e-cash to be transferred as payment.
- $e_s(m)$ : Message  $m$  symmetrically encrypted using secret key  $s$ .
- $d_s(g)$ : Encrypted message  $g$  decrypted using secret key  $s$ .
- $(m)^k$ : Message  $m$  asymmetrically encrypted with a public/private key  $k$ .
- $S_X(m)$ : Message  $m$  digitally signed by  $X$ .
- Share <sub>$i$</sub> : The share of the secret carried by the  $i$ th agent.
- $H(\cdot)$ : One-way collision-free hash function. We will denote  $H(\text{Share}_i)$  as  $H(i)$ .
- *Agent*: A leader agent used to organize the transfer of the shares, any of the mobile agents carrying a share of the secret can be a leader agent
- $P_x$  and  $V_x$ : The public/private key pair of party  $x$ .



- $F_{REC}$ ,  $F_{SUB}$ ,  $F_{CON}$ : Flags used to identify the steps of transferring the shares in the protocol. They indicate the intended purpose of a (signed) message.  $F_{REC}$ ,  $F_{SUB}$ , and  $F_{CON}$  indicate that the objective of the step is transferring a receipt, submitting a document, and confirming the receipt of a document, respectively.
- TTP: On-line trusted third party providing security services accessible to the public.

The steps of the two core phases are described below.

#### 7.4.4 Distribution Phase

The steps of this phase are as follows:

##### 1. Distribute the secret keys using a secret sharing scheme

The customer distributes  $s$  using the secret sharing scheme, an  $(m, n)$  threshold scheme. For this purpose an arbitrary polynomial of degree  $m-1$  is generated:

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{m-1}x^{m-1}, \text{ where } a_0 = s.$$

The coefficients  $a_1, a_2, \dots, a_{m-1}$  are chosen randomly from the set  $Z_p = \{0, 1, \dots, p-1\}$  and are kept secret and discarded after the shadows are handed out.  $p$  is a prime larger than the number of possible shadows (shares), and the largest possible secret. All arithmetic is done modulo  $p$ .

The  $n$  shadows are obtained by evaluating the polynomial at  $n$  random different points,  $y_i = f(x_i)$ . The values of  $x_i (i = 1, \dots, n)$  are made public whereas  $y_i (i = 1, \dots, n)$  are kept secret and act as the  $n$  shares  $\text{share}_i (i = 1, \dots, n)$ .

It is easy to see that when any  $m$  shadows come together, linear algebra can be used to solve for the coefficients of the polynomial, including the constant term,  $a_0 = s$ .

##### 2. Compute $n$ message digests for $n$ shares

A hash function is used to compute  $H(i) = H(\text{share}_i)$ ,  $i = 1, \dots, n$ .

### 3. Prepare $n$ mobile agents

The customer creates  $n$  agents, each agent assigned a unique name  $Agent_i$  ( $i = 1, \dots, n$ ), and will carry the encrypted e-cash  $e_s(C)$ , a share of the secret  $s$ , and a set of  $n$  ordered pairs  $\{x_j, H(j)\}$ ,  $j = 1, \dots, n$ .

### 4. Dispatch $n$ mobile agents to $n$ hosts

The  $n$  agents are dispatched to  $n$  distinct hosts. Each agent will carry the following information:

$$Agent_i, e_s(C), share_i, \{Agent_j, x_j, H(j), j = 1, \dots, n\}.$$

### 5. Register the location of these $n$ mobile agents

After dispatching a mobile agent, the customer's site should register at the name server for the new location of the dispatched mobile agent. The name server maintains a hash map, each record of which is a pair, the agent name and the location. The location consists of a hostname and a port number. It can be resolved using the domain name server (DNS). The agent name is unique, so that the customer and other mobile agents can communicate with it or control it while it travels on its itinerary. So the content of the hash map is:

$$\{Agent_i, Location (Hostname : PortNumber)\}.$$

#### 7.4.5 Payment Phase

The payment phase begins when one of the mobile agents of the customer initiates the payment process after receiving the payment order from the merchant. This agent will be designated as the leader agent or *Lagent*. The payment order (PO) consists of a number of components, as given below:

$$PO = S_M(Tid, Lagent, M, Goods\_desc, Amount, Time)$$

where

$Tid$  = unique identifier for the transaction being carried out,  
 $Goods\_desc$  = description of the goods being purchased,  
 $Amount$  = the amount to be paid to the merchant,  
 $Time$  = the time when the payment order is made,  
 $S_M(message)$  = indicates that the message is signed by  $M$ .

The *Lagent* will randomly select the other  $m-1$  mobile agents and send the payment order signed by the merchant. After the other  $m-1$  mobile agents have verified the payment order, they will send their shares to the merchant. The merchant sends a signed acknowledgment to *Lagent* after the merchant has received  $m-1$  shares. The *Lagent* then sends the last share to a TTP from which the merchant collects it.

The steps of this phase are explained below.

### 1. Initialization

The *Lagent* randomly selects  $m-1$  Agents from the information it carries, finds the locations of these  $m-1$  mobile agents from the *name server*, and sends the following information to the selected mobile agents: the message digest of its share  $\{x_j, H(j)\}$ , the merchant identity  $M$ , and the payment order signed by  $M$ .

Other mobile agents can authenticate *Lagent* using the message digest. They verify the payment order using the merchant's public key. If anything inconsistent is found, the payment is stopped and the problem is reported to the owner.

### 2. Other $m-1$ mobile agents send shares to the merchant

All the selected mobile agents send their shares of the secret key to the merchant:

$$Agent_i \rightarrow M : (Tid, Share_i, x_i)^{P_M} .$$

### 3. Merchant sends the acknowledgement to *Lagent*

After  $m-1$  shares have been received by the merchant, the merchant computes the message digests of the  $m-1$  shares using the same hash function  $H(\cdot)$ . Then the merchant sends the following message as a receipt to *Lagent*:

$$M \rightarrow Lagent : S_M \{F_{REC}, Tid, M, Lagent, m-1 \text{ pairs } (x_i, H(i))\} .$$

### 4. *Lagent* sends its share as the last share to the TTP

*Lagent* verifies that each share received by the merchant is valid by comparing each message digest in the receipt with the one carried by itself. After that *Lagent* sends the  $m$ th (or last) share to the TTP.

$$Lagent \rightarrow TTP : (F_{SUB}, Tid, Lagent, M, e_s(C), Share_m, x_m)^{P_{TTP}} .$$

### 5. *M* and *Lagent* retrieve the confirmed message from the TTP

Both *Lagent* and *M* have to retrieve the confirmed message from the TTP as part of the non-repudiation evidence required in a dispute. It is assumed that even in the case of network failures, both parties will eventually be able to retrieve the message from the TTP.

$$\begin{aligned} M &\leftrightarrow TTP : (F_{CON}, Tid, Lagent, M, e_s(C), Share_m, x_m)^{V_{TTP}}, \\ Lagent &\leftrightarrow TTP : (F_{CON}, Tid, Lagent, M, Share_m, x_m)^{V_{TTP}}. \end{aligned}$$

The two-sided arrow ( $\leftrightarrow$ ) indicates that the transfer is initiated by the recipient through an ftp call.

### 6. Reconstruction of the secret key

Once the merchant gets all  $m$  shares, they reconstruct the secret key  $s$  using the Lagrange interpolation formula:

$$s = a_0 = \sum_{j=1}^m Share_j \prod_{l \leq k \leq m, k \neq j} \frac{x_k}{x_k - x_j}. \quad (1)$$

### 7. Payment

The merchant decrypts the e-cash using  $C = d_s(e_s(C))$ , signs the e-cash with the merchant's private key  $V_M$ , and forwards it to the bank.

#### 7.4.6 Correctness of the Protocol

We show that the secure payment protocol (SPP) presented above provides adequate protection under the threat model presented in the previous section. We do so through a couple of simple claims.

**Claim 1.** The protocol SPP ensures that the e-cash is protected against spying/stealing by  $m - 1$  or fewer malicious MA hosts.

**Proof.** The e-cash is protected by encryption and it requires at least  $m$  agents to reconstruct the encryption key. Since all the transfers take place through secure

channels, and at no point of the protocol has any one agent access to more than one share, this property is trivially guaranteed provided that the agent itinerary ensures that no MA host is ever visited by more than  $m - 1$  agents.

Note that the protocol will fail if there is collusion between the merchant and the host of *Lagent*.

Since the merchant receives  $m - 1$  shares from the other  $m - 1$  agents, the merchant simply needs to pass them to the host of the *Lagent*, who then uses that information to extract the e-cash.

**Claim 2.** The protocol produces evidence to support non-repudiation for both the customer and the merchant.

**Proof.** The nonrepudiable evidence is generated at steps 3, 4, and 5 of the payment phase. At step 3, the merchant signs and sends message digests of the  $m - 1$  shares already received by them. If these digests are not all valid, the *Lagent* will not complete the payment. If they are valid, they serve as evidence of M's receipt of the  $m - 1$  shares.

In step 4, the *Lagent* passes the last share as well as the encrypted e-cash to the TTP. This message is protected by encryption using the public key of the TTP. This ensures that the merchant cannot spy on the last share from this message.

This message need not be signed by *Lagent* as the TTP is trusted. (Otherwise it could have passed the message clandestinely to the merchant, later corrupting the data and producing untenable non-repudiation evidence.)

In step 5, both M and *Lagent* retrieve the message using ftp, which serves as the non-repudiable evidence of transfer of the last share as well as the e-cash.

In summary, at the end of this protocol, if *Lagent* wants to prove that the shares have been received, it presents

$$S_M(F_{REC}, Tid, M, Lagent, m-1 \text{ pairs } \{x_i, H(i)\})$$

and  $(F_{CON}, Tid, Lagent, M, e_s(C))$

to the judge. The first piece of evidence confirms that *M* received the  $m - 1$  shares, and the second piece confirms that the last share was deposited with the TTP, which means that the merchant has access to it.

#### 7.4.7 Efficiency of the Protocol

The message complexity of the protocol can be computed as follows. In the initialization phase, the *Lagent* sends  $m-1$  messages of  $O(1)$  length to  $m-1$  participating agents. Each of the agents transfers its share to the merchant, using altogether  $m-1$  messages of  $O(1)$  length.

The merchant sends the single acknowledgement message of length  $O(m-1)$  in step 3. In steps 4 and 5, three messages are transmitted, each of length  $O(1)$ . Thus altogether, the complexity of the messages communicated is  $3O(m-1)+3O(1)$ , whereas the total number of messages transferred is  $3(m-1)+3=3m$ .

The parameter  $m$  can be viewed as a measure of untrustworthiness of the host network. Therefore, it can be said that the cost of protection increases linearly with the number of untrustworthy hosts in the network. The secret key is distributed to  $n$  shares,  $m$  of them is enough to reconstruct the secret,  $n \geq m$ .

The larger  $m$  and  $n$  are, the more secure and reliable the protocol is. But at the same time, the cost increases. To select  $m$  and  $n$  one needs to find a good balance among the safety, reliability, cost, and efficiency of the protocol.

It is worth noting here that the protocol involves the TTP only for the transfer of the last share. So the TTP remains unaffected by the choice of  $m$ .

#### 7.4.8 Limitations of the Protocol

The protocol discussed above is a very basic one and has several drawbacks that must be addressed effectively before it can be put to practical use. First of all, since the secret key is revealed at the end of each payment operation, the protocol requires a different key to be used for each payment transaction.

Second, since the value of the e-cash token is fixed at creation, this protocol cannot be used in cases where the amount to be paid is not known before the creation of the mobile agents.

Third, there are important additional security issues that need to be addressed. For example, if  $m$  or more of the mobile agents pass through any given untrusted host in the course of their nomadic lifetime, that host can gather all the information necessary to reconstruct the secret. To avoid this possibility, one can either preplan the itineraries of all the mobile agents or the mobile agents need to consult a central controlling agent for clearance to move to an intended site.

Another possible attack can be mounted in which a malicious host that hosts any one agent creates a fake merchant identity and makes up a payment order in which it makes itself the recipient site. However, any payment protocol is vulnerable to such an attack, and the only effective way to address this is by making the certification process more reliable.

#### 7.4.9 An Electronic-Check-Based Payment Protocol

The constraints imposed by the SSP protocol presented above, namely the single use of secret keys and the predetermined amount of the payment can be removed with some modifications if the requirement for anonymity is given up. In what follows, we describe a modified version of the SSP protocol that uses electronic checks rather than e-cash and thus no longer provides anonymity to the customer.

The exposure of the secret key at the end of each transaction can be avoided by using a homomorphic secret sharing scheme [7.19]. We can partition the private key in a way that each mobile agent can partially encrypt or sign the message without revealing their share to the combiner. After the last partial signature, the document is completely signed with the shared private key, and none of the shareholders learns about any other shares. The combiner can get the whole signature after each mobile agent has signed without knowing the private key. This concept is explored further in [7.20].

Let  $g$  be an encryption function, if  $g$  is homomorphic it satisfies the following equation:

$$g(k_1 + k_2) = g(k_1) \times g(k_2). \quad (2)$$

If  $k_1 + k_2$  is the encryption key, then a threshold cryptographic system may be constructed [7.21]. As an example, in computing an RSA signature one computes  $g_h(s) = h^s \bmod n$ , where  $h = H(\text{message})$  is the message digest,  $s$  is the secret key,  $n = p \times q$  is the public modulus, and  $p$  and  $q$  are two distinct large primes. From (1), and with careful choice of  $p$  and  $q$ , Shamir's scheme satisfies the property

$$s = \sum_{i \in Q} (\text{constant}_{i,Q} \times s_i), \quad (3)$$

where  $Q$  is a quorum subset of the set of all participants, called  $A$ , and  $|Q| = m$  is the threshold value. From (1), the terms  $\text{constant}_{i,Q}$  can be obtained from the known values of  $x_i$  as follows:

$$\text{constant}_{i,Q} = \prod_{k \in Q, k \neq i} \frac{x_k}{x_k - x_i}. \quad (4)$$

Hence, when combined with a homomorphic  $g$ , one obtains:

$$\begin{aligned} g_h(s) &= g_h \sum_{i \in Q} \text{constant}_{i,Q} \times s_i \\ &= \prod_{i \in Q} g_h(\text{constant}_{i,Q} \times s_i) \\ &= \prod_{i \in Q} g_h(s_i)^{\text{constant}_{i,Q}} \end{aligned} \quad (5)$$

Thus, an RSA signature can be computed using partial signatures, yet both the private key  $s$  and the various shadows remain secret even after combining the shares.

The payment protocol based on e-check is described briefly in the following steps:

- Step 1.** The customer first distributes her private key  $s$  using a polynomial of degree  $m-1$ , and gets  $n$  shadows  $s_i$  by evaluating the polynomial at  $n$  different points  $x_i$ . The customer creates  $n$  mobile agents with  $\{x_i, s_i\}$  and dispatches them to  $n$  different hosts through secure channels.
- Step 2.** Whenever any of the customer agents, say  $agent_j$ , wishes to make a payment against a properly authenticated payment order sent by the relevant merchant, it creates an e-check  $C$  of an appropriate amount, computes  $h = H(C)$  and then a partial signature  $g_h(s_j)$ . The agent sends  $\{C, g_h(s_j), x_j\}$  along with proper identifiers to the merchant through a secure channel. At the same time it sends the payment order and a copy of the check  $C$  to randomly selected  $m-1$  other customer agents.



**Step 3.** All the  $m-1$  customer agents that receive the above message generate their own partial signature  $g_h(s_i)$  and send  $\{g_h(s_i), x_i\}$  along with proper identifiers to the merchant through a secure channel.

**Step 4.** After collecting  $m$  partial signatures, the merchant combines them to obtain the fully signed e-check  $g_h(s)$  using the formula given in (5).

Note that a TTP can be involved if a non-repudiation service is needed. In this case, the leader agent will send its partially signed check through the TTP instead of sending it directly to the merchant and a protocol similar to the one described using e-cash can be used to ensure proper documentation.

It may be noted that since this protocol involves the signature of the customer, it does not support the anonymity of the customer.

#### **7.4.10 Possibility of Combining Anonymity with Reuse of Secret Key by Payment Agent**

To protect a payment agent from malicious usurpation, one must ensure that no agent ever has complete knowledge of a validated instrument of payment, such as cash or a signed check. As we have seen in the preceding section, using a threshold encryption scheme, a set of mobile agents can generate an e-check of arbitrary amount independently of any intervention by the owner and can complete payment in a secure manner. However, this process requires the customer agents to give up anonymity. The question is whether it is possible to combine the flexibility of making payments in arbitrary denominations a multiple number of times using a single secret key while retaining anonymity. With the available cryptographic techniques that seems to be impossible at the time being. Whether it is possible at all is debatable, and it is best to withhold any conclusion until it is proven formally either way.

### **7.5 Summary**

In this chapter, we have addressed the problem of protecting sensitive information carried by mobile agents from malicious hosts, and proposed two payment protocols using Shamir's secret sharing scheme. One of the protocols is based on electronic cash that allows the customer to carry out transactions anonymously. But it imposes two constraints, namely, the amount to be paid must be predetermined, and secondly for each payment transaction a new secret key needs to be used. The second protocol, which is based on electronic check payment, removes these constraints at the cost of anonymity. The protocols guarantee protection of confiden-

tial data, such as electronic cash, against concerted attack by a known maximum number of malicious hosts. In addition, by making optional use of a TTP in a minimal way, it produces non-repudiable evidence of transfer of funds from the customer to the merchant.

## 7.6 References

- [7.1] A. Chavez, P. Maes (1996) Kasbah: an agent marketplace for buying and selling goods. In: Proceedings of the First International Conference on the Practical Application of Intelligent Agents and Multi-agent Technology.
- [7.2] J. G. Lee, J. Y. Kang, E. S. Lee (1997) ICOMA: an open infrastructure for agent-based intelligent electronic commerce on the Internet. In: Proceedings of the International Conference on Parallel and Distributed Systems.
- [7.3] P. Maes, R. H. Guttman, A. G. Moukas (1999) Agents that buy and sell: transforming commerce as we know it. *Comm ACM* (March Issue).
- [7.4] A. Moukas, R. Guttman, P. Maes (1998) Agent-mediated electronic commerce: an {MIT} media laboratory perspective. In: Proceedings of ICEC Conference, 1998.
- [7.5] M. Tsvetovatyy, M. Gini (1996) Toward a virtual marketplace: architectures and strategies. In: Proceedings of the First International Conference on the Practical Application of Intelligent Agent and Multi-agent Technology (PAAM'96), Blackpool, 1996.
- [7.6] M. Tsvetovatyy, M. Gini, B. Mobasher, Z. Wieckowski (1997) MAGMA: an agent-based virtual market for electronic commerce. *J Appl Artificial Intelligence*.
- [7.7] A. Young, M. Yung (1997) Encryption tools for mobile agents: sliding encryption. In E. Biham (ed.) *Fast software encryption – FSE'97*, LNCS 1267. Springer, Berlin Heidelberg New York.
- [7.8] F. Hohl (1997) An approach to solve the problem of a malicious host. Report No. 1997, Universität Stuttgart, Fakultät Informatik.
- [7.9] T. Sander, C. Tschudin (1997) Towards mobile cryptography. Technical Report, International Computer Science Institute, Berkeley.
- [7.10] T. Sander, C. Tschudin (1997) Protecting mobile agents against malicious hosts. In: *Mobile agent security*, Springer, Berlin Heidelberg New York.
- [7.11] M. Bellare, P. Rogaway (1994) Optimal asymmetric encryption. In: *Eurocrypt 94*, LNCS 950. Springer, Berlin Heidelberg New York.
- [7.12] R. Rivest, A. Shamir, L. Adleman (1978) A method for obtaining digital signatures and public key cryptosystems. *Commun ACM* 21(2): 120–126.

- [7.13] A. Das, G. Yao (2001) A secure payment protocol using mobile agents in an untrusted host environment. In: W. Kou, et al. (eds.) Electronic commerce technologies – ISEC 2001, LNCS 2040. Springer, Berlin Heidelberg New York.
- [7.14] G. Yao (2001) Security mechanisms for mobile agent-based e-commerce systems. Master's Thesis, Nanyang Technological University.
- [7.15] A. Shamir (1979) How to share a secret. Commun ACM 22:612–613.
- [7.16] D. Chaum (1989) Online cash checks. In: Proceedings of Advances in Cryptography–Eurocrypt'89, LNCS 434. Springer, Berlin Heidelberg New York.
- [7.17] S. A. Brands (1993) An efficient off-line electronic cash system based on the representation problem. Technical Report CSR9323, Computer Science Department, CWI, US.
- [7.18] S. Brands (1994) Untraceable off-line cash in wallet with observers. In: Advances in Cryptology–CRYPTO'93. Springer, Berlin Heidelberg New York.
- [7.19] J. C. Benaloh (1997) Secret sharing homomorphisms: keeping shares of a secret secret. In: A. Odlyzko (ed.), Advances in Cryptology, Proc. of Crypto'86, Santa Barbara, CA, US, Aug. 1987.
- [7.20] Y. Desmedt (1997) Some recent research aspects of threshold cryptography. In: E. Okamoto, et al. (eds.), Information security, LNCS 1396. Springer, Berlin Heidelberg New York.
- [7.21] N. Jacobson (1985) Basic algebra, I.W.H. Freeman, New York.

## 8 Digital Cash

Yi Mu<sup>1</sup>, Vijay Varadharajan<sup>1</sup>, and Khanh Quoc Nguyen<sup>2</sup>

<sup>1</sup> Department of Computing, Macquarie University,  
Sydney, Australia

<sup>2</sup> Gemplus Technologies Asia,  
12 Ayer Rajah Crescent, Singapore

### 8.1 Introduction

A digital-cash system normally consists of clients, vendors, and a bank. Any legitimate client can obtain a valid digital coin<sup>1</sup> from a bank and anonymously send the coin to a vendor. The vendor later deposits the coin to the bank. Because of the anonymity of the client, the bank can validate the coin but cannot link the coin to the information used in the coin-issuing process. The bank and the vendor cannot trace transactions made by the client.

The first digital-cash scheme was proposed by Chaum [8.1]. The transaction untraceability proposed in Chaum's digital-cash is based on the use of zero-knowledge proofs, which is computationally expensive and is not efficient enough for any real applications. Some subsequent works [8.2, 8.3, 8.6, 8.7] have achieved various improvements on Chaum's scheme. In particular, protocols proposed by Brands [8.2] and Ferguson [8.6] achieve transaction untraceability without requiring zero-knowledge proofs.

There are several forms of digital-cash. Besides the normal digital-cash, there are two additional catalogs: divisible digital-cash and fair digital-cash.

The first divisible digital-cash scheme was proposed by Okamoto [8.7], and then two more efficient methods were proposed [8.8, 8.9]. The divisible digital-cash scheme allows a user to divide a digital coin into several even

---

<sup>1</sup> For convenience, we use "digital coin" to represent a monetary unit of digital cash.

pieces that can be used as normal digital coins. Fair digital-cash schemes are applied to restricting unconditional privacy of clients. In a normal digital-cash system, there is no any mechanism for banks and vendors to identify a client in a transaction without breaking the underlying number theoretic assumptions. This protection, which is desirable from client's viewpoint, is a major concern for law enforcement agencies. It was pointed out in [8.16, 8.31] that anonymous e-cash can be a "safe haven" for criminal activities that include money laundering, illegal purchases, perfect blackmailing and other attacks. This prevents the deployment of anonymous digital-cash cash systems in a large scale, where such attacks and many others are often expected. In a fair digital-cash system, a designated trusted third party can compute the identity of a client when necessary.

In this chapter, we will introduce three typical digital-cash schemes: the digital-cash scheme proposed by Brands [8.2], and the digital-cash and the fair digital-cash scheme proposed by Nguyen et. al. [8.14, 8.14].

## 8.2 Security Requirements for Digital Cash

Digital-cash must not be illegally forgeable and cannot be double spent. In the meanwhile, digital-cash must also have such properties as providing anonymity to clients and untraceability to digital coins. In general, Digital-cash should have the following security properties:

- **Unforgeability.** This is the basic requirement for digital-cash. Digital cash must not be able to be forged in a polynomial time frame.
- **Untraceability.** Once a digital coin is issued, it is not traceable by the bank and any other parties.
- **Anonymity.** The identity of the digital-cash owner should not be revealed. That is, given a digital coin, any other parties cannot find the identity of the owner.
- **Double-spending detection.** A digital coin can be used only once, bounded by its monetary value. Any attempt at duplication of a coin or double uses of a coin can be detected by the bank that has signed the coin.
- **Fairness.** In fair digital-cash, the anonymity of a coin owner is conditional. There is a trusted third party who can find the identity of the coin owner when the coin has been illegally used.

### 8.3 Brands' Digital-Cash Scheme

Brands proposed the first digital-cash scheme without using cut-and-choose, therefore it is much more efficient than Chaum's original scheme. In this section, we introduce Brands' scheme. Like Chaum's scheme, Brands' digital-cash scheme has four phases: opening an account, withdrawal, payment, and deposit. For simplicity of the following presentation, we have slightly modified the scheme without compromising its security.

#### 8.3.1 The Setup

We first give some general notations to be used in Brands' digital-cash scheme.

- $p$ : a large prime
- $q$ : an integer satisfying  $q|p - 1$
- $\mathbb{Z}_p^*$ : a multiplicative group of prime order  $q$  satisfying  $q|p - 1$
- $\mathbb{G}_q$ : a multiplicative group of prime order  $q$  and  $\mathbb{G}_q \subset \mathbb{Z}_p^*$
- $\mathbb{Z}_q$ : a finite field of size  $q$
- $\mathcal{H}(\cdot)$ : a strong correlation-free one-way hash function  $\mathcal{H}(\cdot) \in \mathbb{Z}_q$

The system consists of clients, merchants, and a bank. We denote by  $C$  a client,  $M$  a merchant, and  $B$  a bank.

$B$  chooses  $(g_1, g_2, g_3) \in_R \mathbb{G}_q^3$  as generators and a number  $x \in_R \mathbb{Z}_q$  as its private key, and then computes its public key  $z = g^x \bmod p$ . For simplicity, we will omit modulo  $p$  in the following protocols.

#### 8.3.2 Opening an Account

To open an account,  $C$  and  $B$  follow the following steps:

1. The client  $C$  needs to identify himself to the bank  $B$ , when opening an account by, for example, showing his passport to  $B$ .
2.  $C$  selects a secret random number  $U \in_R \mathbb{Z}_q$  and computes  $I = g_1^U$  where  $g_1^U g_2 \neq 1$ , then sends  $I$  to  $B$ .
3.  $B$  stores  $C$ 's identification information along with  $I$ .  $I$  will be used as  $C$ 's account number.

The security of  $U$  is based on the difficulty of solving discrete logarithm. In other words, if  $C$  spends a digital coin related to  $I$  once, his identity  $U$  cannot be computed within a polynomial time frame.

**8.3.3 The Withdrawal Protocol**

To withdraw a coin from  $B$ ,  $C$  needs first identify himself to  $B$  and prove his ownership of the account. The following withdrawal protocol is then performed (also see Fig. 8.1).

1.  $B$  generates a number  $w \in_R \mathbb{Z}_q$  and sends  $a = g^w$  and  $b = (Ig_2)^w$  to  $C$ .
2.  $C$  generates three numbers  $s, x_1, x_2 \in_R \mathbb{Z}_q$  and computes  $A = (Ig_2)^s$ ,  $B = g_1^{x_1} g_2^{x_2}$ , and  $z' = z^s$ .  $C$  also generates two numbers  $u, v \in_R \mathbb{Z}_q$  and uses them to compute  $a' = a^u g^v$  and  $b' = b^{su} A^v$ .  $C$  then computes the challenge  $c' = \mathcal{H}(A, B, z', a', b')$ , and sends the blinded challenge  $c = c'/u \bmod q$  to  $B$ .
3.  $B$  sends the response  $r = cx + w \bmod q$  to  $C$ , and debits the account of  $C$ .

$C$  accepts iff  $g^r = h^c a$  and  $(Ig_2)^r = z^c b$ . If this verification holds,  $C$  computes  $r' = ru + v \bmod q$ . The withdrawn coin consists of  $(A, B, z', a', b', r')$ .

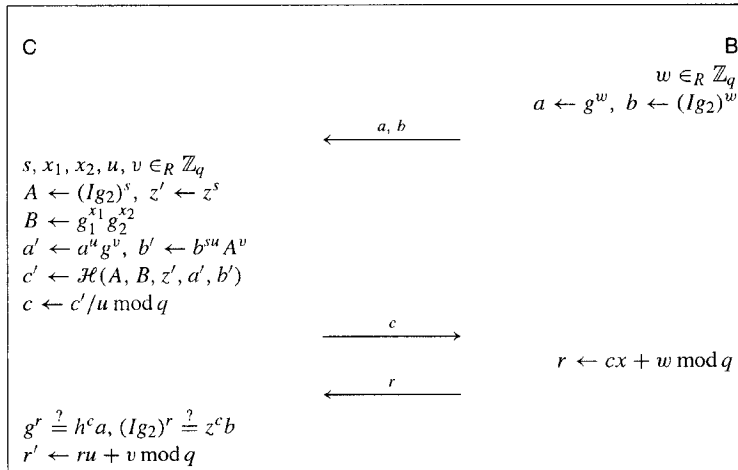


Fig. 8.1 The coin withdrawal protocol

**8.3.4 The Payment Protocol**

When  $C$  wants to spend his coin at  $V$ , the following protocol is performed.

1. C sends  $A, B$ , and  $\text{Sign}(A, B)$  to V, where  $\text{Sign}(A, B)$ , which represents B's signature on a pair  $(A, B) \in (G_q)^2$ , is the tuple  $(A, B, z', a', b', r')$ .
2. V computes a challenge  $d = \mathcal{H}_0(A, B, ID_V, \text{Date/Time})$  and sends  $d$  to C.
3. Upon receipt of  $c$ , C computes the responses  $r_1 = du_1s + x_1 \bmod q$  and  $r_2 = ds + x_2 \bmod q$ , and then sends them to C.

V accepts the coin iff  $\text{Sign}(A, B)$  is valid and  $g_1^{r_1} g_2^{r_2} = A^d B$ .

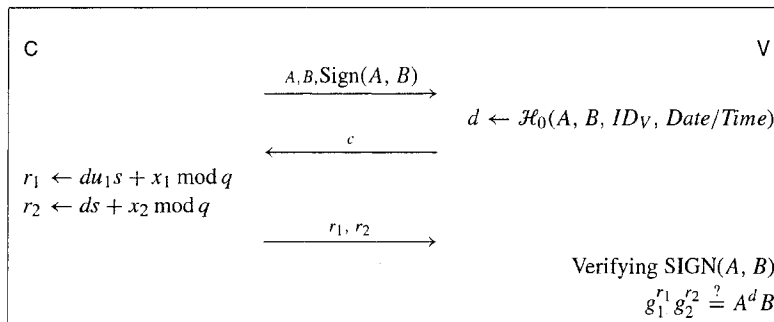


Fig. 8.2 The payment protocol

### 8.3.5 The Deposit Protocol

V sends the payment transcript of a coin to B. B needs to check if the coin has been stored before. If not, B stores  $(A, \text{Date/Time}, r_1, r_2)$  in its database as being deposited by V, and credits the account of V. However, if the coin has been spent before, a double-spending fraud must have occurred. A double-spending can be easily detected, since the challenges are different. B can obtain a triplet  $(c, r_1, r_2)$  from the new transcript and a triplet  $(c', r'_1, r'_2)$  from the deposited information. B can compute  $I = g_1^{(r_1 - r'_1)/(r_2 - r'_2)}$  and then search its database for this account number.

### 8.4 One-Response Digital Cash

Current offline digital-cash systems [8.1, 8.4, 8.6] tend to provide double-spending detection, client anonymity, and transaction untraceability. However, as there is always a trade-off between double-spending detection and transaction untraceability, the computational cost is often high. Even in the most efficient systems [8.4, 8.6], many discrete exponential computations are required for each digital monetary unit in order to achieve the untraceability. To design an electronic-payment system that



allows small payment amounts, heavy use of discrete exponential computations must be avoided. In fact, this requirement makes all current offline cash systems economically infeasible.

In this section, we introduce an efficient approach [8.13] to offline digital-cash schemes that makes small payment amounts possible. This scheme maintains the basic features in digital-cash: client anonymity and double-spending detection. The computational efficiency achieved in this scheme is due to the use of one-way hash functions that make clients perform only *one* major computation and perform no discrete exponential computations in the payment phase. This feature leads to a significant improvement in computational efficiency in contrast to all previously proposed schemes.

#### 8.4.1 Schnorr's One-Time Signature Scheme

Schnorr's one-time signature scheme [8.11] is used for this digital-cash scheme. Let  $p$  and  $q$  be prime such that  $q$  is a prime factor of  $p - 1$ . Let  $g \in \mathbb{Z}_p^*$  be the multiplicative primitive, where  $g \neq 1$  and  $g^q \equiv 1$ . Again, we omit the modulo  $p$  in our presentation.

To generate a particular pair of private key and public key, a user (say, Alice) chooses a random number  $s$  as her private key,  $0 < s < q$ . Alice then computes her public key  $v$  as  $v = g^{-s}$ .

To sign a message  $m$ , Alice picks a random number  $r \in \mathbb{Z}_q$  and does the following computations:

$$\begin{aligned} x &= g^r \\ c &= \mathcal{H}(m \| x) \\ y &= (r + sc) \bmod q, \end{aligned}$$

where  $\mathcal{H}(\cdot)$  is a suitable collision-free one-way hash function. The signature on the message  $m$  is the pair  $(c, y)$ . To verify the signature, we check:  $x \stackrel{?}{=} g^y v^c$  and check if  $c$  is equal to  $h(m \| x)$ .

#### 8.4.2 The One-Response Digital-Cash Protocol

We assume that each *coin* in this scheme represents a monetary unit. The face value of each coin is decided by the bank. We denote by  $C_i$  a coin with an abstract face value  $c_i$ . We also assume that the bank has a RSA public/secret key  $(e, d)$  with the composite modulo  $n$  of the product of two large prime numbers,  $q_1, q_2$ , and a number  $g$  such that  $g^q \equiv 1$  and  $\gcd(g - 1, n) = 1$ . The values of  $g, p, q, n$ , and  $e$  are public.

**Account opening phase.** When C wishes to open an account at B, after identifying himself to B, C uses a zero-knowledge process to obtain a blind-signature from B on  $h(g^U)$  as  $(h(g^U))^d \bmod n$ .  $U$  is constructed as  $U = I\|k$  ( $0 < U < q$ ) by C, where  $\|$  denotes a concatenation of bits,  $k$  is a random number, and  $I$  is the client identity registered with the bank (also referred as the client's bank account number). The bank should not have any knowledge about the value of  $k$  and consequently the value of  $U$ . There have been several such zero-knowledge processes<sup>2</sup> described in the literature; see, for instance, [8.12, 8.10].

The length of  $I$  and  $k$  should be fixed, at least 80 bits each, so that given  $g^U$ , it is feasible to obtain  $I$ . After the account's opening phase, the client has an anonymous bank certificate  $Cert$  as  $(h(g^U))^d \bmod n$ . This certificate would remain anonymous as long as nobody is able to compute  $U$ . Extracting  $U$  from  $Cert$  is infeasible unless the client double-spends under the discrete logarithms assumption (Further discussions will be given later.) After the account-opening process, C stores  $Cert$  and  $g_C = g^U$ .

**Withdrawal phase.** Before withdrawing any money from the bank, the client C proves his ownership of  $I$  to B. If the client wishes to withdraw  $k$  coins, he chooses a random number  $c_k$  and computes  $c_i = h(c_{i+1})$  for  $\forall i \in \{1, \dots, k - 1\}$ . For each  $c_i$ , C uses a blind signature technique[8.5] to withdraw an anonymous coin from B using the following protocol (see Fig. 8.3):

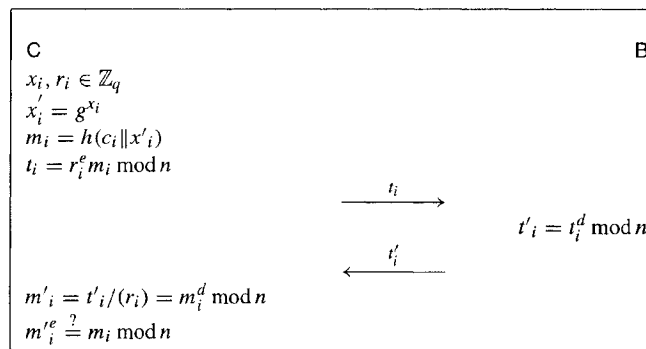


Fig. 8.3 The withdrawal protocol

<sup>2</sup> A cut-and-choose method has to be used in the proof. To avoid it, a trusted third party may be included for verifying correctness of  $h(g^U)$  and signs it prior to the bank's signing.

1. C generates a random number  $x_i \in_R \mathbb{Z}_q$ , and computes:  $x'_i = g^{x_i}$ ,  $m_i = h(c_i \| x'_i)$ .
2. C then uses blind signature technique [8.5] to obtain a bank signature on  $m_i$  by choosing a blind factor  $r_i$  and sending  $t_i = r_i^e m_i \bmod n$  to B. B signs the value of  $t_i$  and returns the signature as  $t'_i$ . The client then removes the blind factor  $r_i$  to obtain the bank blind signature  $m'_i = t'_i / r_i = m_i^d \bmod n$ .

For each signature, the bank deducts the client's account by an equivalent value of a coin. After the withdrawal, C has each coin  $C_i$  with a face value of  $c_i$  in the form of  $[h(c_i \| x'_i)]^d \bmod n$ . It is unforgeable unless the factorisation of  $n$  is known.[8.1] For each coin  $C_i$ , C stores  $[c_i, x_i, x'_i, m'_i]$ .

**Payment phase.** When the client wants to spend the coin chain  $C_1, C_2, \dots, C_n$  to V, he must spend them in the order  $C_1, C_2, \dots, C_n$ .

Without the loss of generality, we assume that C has already spent all the coins  $C_0, C_1, \dots, C_{i-1}$  in some previous payments. Now if C wishes to pay some coins to V, C must send the coins to V in the exact sequence  $C_i, C_{i+1}, \dots, C_j, \dots$  according to the following process:

- For the first coin  $C_i$  (see also Figure 8.4):
  1. V generates a random challenge  $a$  and sends it to C. This challenge should be unique for each transaction. For example, it can be computed as  $a = h(C \| V \| Date \| Time)$ .
  2. C computes the response  $b = x_i - Ua \bmod q$  for the challenge  $a$  and sends it along with  $(Cert, g_C, b, c_i, x'_i, m'_i)$  to V. The response  $b$  is also considered as Schnorr's one-time signature on the message  $a$ , where  $x_i$  is a one-time value.

V accepts the coin if and only if  $Cert$  and  $m'_i$  are valid bank signatures on  $g_C$  and  $\mathcal{H}(c_i \| x'_i)$ , respectively, and  $g_C^a g^b = x'_i$ .

- For every coin  $C_j$ , thereafter (see also Fig. 8.5):

C sends  $(x_j, c_j, m'_j)$  to V. V accepts the coin  $C_j$  if and only if  $h(c_j) = c_{j-1}$  (where  $c_{j-1}$  was obtained from the previous coin) and  $m'_j$  is a valid bank signature on  $h(c_j \| g^{x_j})$ .

For the sake of convenience, let us name the first coin  $C_i$  as *signed coin* and all the other coins  $C_j$  as *normal coins*.

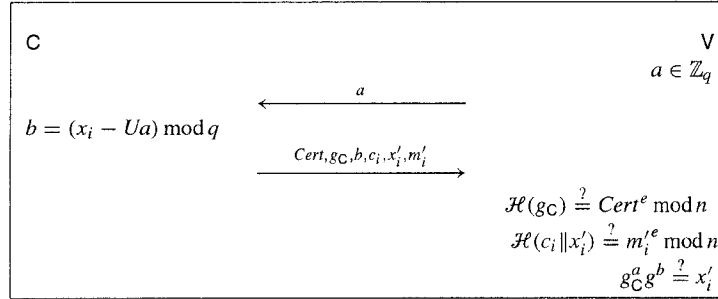


Fig. 8.4 The payment protocol for the first coin

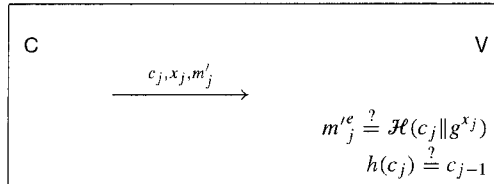


Fig. 8.5 The payment protocol

**Deposit phase.** In deposit phase, V deposits all the received coins at B by sending  $(Cert, g_C, a, b, c_i, x'_i, m'_i)$  for each signed coin and  $(c_j, x_j, m'_j)$  for each normal coin. B goes through exactly the same verification process as V did in the payment phase. If everything is OK, B pays V an equivalent amount of money and stores  $(a, b, c_i)$  for the first coin,  $(c_j, x_j)$  for each other coin in its coin database.

**8.4.3 Discussion**

In this section, we will closely examine security and efficiency features of the system, including double-spending detection, client anonymity, and efficiency.

**Double spending.** Double-spending occurs when C double spends some coins in the hope that B cannot detect the identity. In our protocol, double-spending is detected as follows:

When C double spends some coins, for the first double-spent coin  $C_i$ , it must be a signed coin in at least one transaction. So there are only two possibilities:  $C_i$  is spent as either a signed coin in the both transactions or as a signed coin in one transaction and as a normal coin in another transaction.

- Double spend a coin as signed coins: C spends  $C_i$  as a signed coin twice, i.e., for two different challenges  $a$  and  $a'$ , B therefore has  $b = x_i - Ua \pmod q$  and  $b' = x_i - Ua' \pmod q$ . B can easily find  $U$  by computing:

$$U = \frac{b - b'}{a' - a} \pmod q$$

- Spend a coin as a signed coin and as a normal coin: C spends  $C_i$  twice, once as a normal coin and the other as a signed coin. B therefore has  $a$  and  $x_i - Ua$  from the signed coin and  $x_i$  from the normal coin. This information is sufficient to compute  $U$ .

So in either case, the value  $U$  can be computed. After obtaining  $U$ , B extracts  $I$  and matches it with the client's ID stored in its database. Once a match is found, B asks C to reveal the value  $U$  incorporated in his  $Cert$ . If this value matches the value  $U$  obtained by B from the first double-spent coin, C must have double spent the coin. The evidence is *undeniable* because  $U$  is client's secret information, which is infeasible for anyone else to compute unless the client had double spent a coin.

**Anonymity.** Client anonymity is protected unconditionally in this scheme. The zero-knowledge process used in the account's opening phase completely hides the identity of the client. The bank will not be able to link  $Cert$  to C's ID, once  $Cert$  is issued. On the other hand, our coins are blindly signed by the bank so the bank cannot trace any particular coin to any particular client.

During the payment process, the client only has to show  $Cert$ , which is an anonymous certificate and reveals  $x_i - Ua \pmod q$  for each signed coin and  $x_j$  for each normal coin. For two different coins, as their corresponding  $(x_i, x_j)$  are chosen at random, they are different and unlinkable. Having only  $a$ , B cannot obtain  $U$  from  $x_i - Ua \pmod q$  (since  $x_i$  is chosen at random).

**Efficiency.** The account's opening phase is a one-off process, so even though the zero-knowledge process is inefficient, it will not affect the efficiency of the system for any transaction later on.

The withdrawal phase is very efficient. To withdraw a coin, ignoring the number of hash operations, C computes only two exponentiations. The number of discrete exponentiations required in Chaum's [8.1], Ferguson's [8.6], Brands' [8.4] protocols are forty, seventeen, and ten, respectively. In contrast to these schemes, this protocol needs only two multiplication operations.

In the payment protocol, for the whole transaction, the client only has to compute a single response, i.e.,  $b = x_i - Ua \pmod q$ . This is far more efficient than all off-line

digital-cash schemes known to date, especially as the response message does not involve any discrete exponential computation. Moreover, the vendor, in the payment phase, does not need to perform any complicated verification. In fact, the vendor only has to verify one RSA signature per coin plus a certification *Cert* and a Schnorr's one-time signature for each transaction.

Hence the protocol is much more efficient than other existing digital-cash schemes such as those in [8.1, 8.4, 8.6, 8.12].

### 8.5 Fair Digital Cash

Brickell, Gemmell, and Kravitz [8.16] proposed an escrowed digital-cash scheme to control unconditional privacy of clients, often known as *fair digital-cash*. The main feature of fair digital-cash is the existence of a trusted authority or a revocation authority that can revoke the anonymity of any given coin. A different and more efficient scheme was later proposed by Camenisch, Piveteau, and Stadler [8.27]. Both schemes require the revocation authority to be actively involved in every withdrawal and thus are not desirable.

Frankel, et. al. [8.25] and Camenisch, et. al. [8.20] respectively proposed a fair digital-cash scheme employing an off-line revocation authority. The advantage of this approach is that the revocation authority is not involved in any payment transaction. When needed, the revocation authority can be called upon to identify the owner of a coin or a transaction. The most efficient schemes to date are those by Davida, Frankel, Tsiounis, and Yung [8.24] and by Camenisch, Maurer, and Stadler [8.20]. Both of these two schemes are constructed from Brands' anonymous e-cash scheme.

In this section, we will not describe all fair-digital-cash schemes, whereas we introduce the concept of fair-digital-cash by using a typical model that uses an off-line revocation authority [8.28]. This fair-digital-cash scheme is based on Nyberg-Rueppel digital signature scheme and thus poses as an alternative to Schnorr-based fair-digital-cash schemes.

In a fair e-cash scheme, there are the following parties, a bank B, a trusted authority T, vendors, and clients. We denote by V a vendor and by C a client.

A fair e-cash scheme consists of five basic protocols, three of them are the same as in anonymous e-cash, i.e., a withdrawal protocol, a payment protocol, and a deposit protocol. The two additional protocols are conducted between B and T, *owner-tracing* and *coin-tracing* protocols.

- In the owner-tracing protocol, **B** gives to **T** the view of a deposit protocol and **T** returns a string that contains some specific information which allows **B** to identify the owner of the coin.
- In the coin-tracing protocol, **B** gives to **T** the view of a withdrawal protocol and **T** returns some specific information that allows **B** to identify the coin in the deposit phase.

These two additional protocols provide the revocation capacity and the protection against certain types of attacks. For instance, the owner-tracing protocol allows the authorities to identify the origin of dubious coins and thus eliminates money laundering. The coin-tracing protocol allows the authorities to find the destination of dubious coins and thus eliminates blackmailing.

In the following, we will first introduce a digital-cash scheme based on Nyberg–Rueppel digital-signature scheme[8.21] and then convert it to a fair version.

### 8.5.1 Nyberg-Rueppel Digital-Signature Scheme

The key generation protocol works as follows. Let  $p$  be a large prime and  $q$  be equal to  $p - 1$  or a large integer factor of  $p - 1$ . Also let  $g$  be a random generator of  $\mathbb{G}_q \subset \mathbb{Z}_p^*$ . Each signer chooses  $x \in_R \mathbb{Z}_q^*$  and computes  $h = g^x \bmod p$ , where  $(x, h)$  is his secret and secret-public key pair. Again, we omit the modulo  $p$  in our presentation.

To sign a message  $m \in \mathbb{Z}_p$ , the signer selects a random number  $w \in \mathbb{Z}_q$  and computes  $r$  and  $s$  as

$$r = mg^w \text{ and } s = xr + w \bmod q.$$

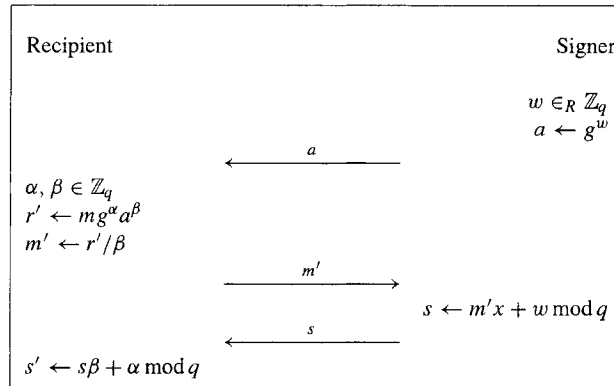
The pair  $(r, s)$  is the signature of the message  $m$ . To verify the signature, we check

$$m = g^{-s} h^r r.$$

This signature scheme can be converted into a blind version using the protocol given in Fig. 8.6.

The pair  $(r', s')$  is a blind signature on message  $m$ . The correctness of the signature is shown as follows:

$$\begin{aligned} g^{-s'} h^{r'} r' &= mg^{-s\beta - \alpha + xr' + w\beta + \alpha} \\ &= mg^{-m'x\beta - w\beta + r'x + w\beta} \\ &= mg^{xr' - xm'\beta} = m. \end{aligned}$$



**Fig. 8.6** Blind Nyberg–Rueppel digital signature scheme

The blindness holds because if  $\alpha$  and  $\beta$  are chosen at random,  $r'$  and  $m$  are uniformly distributed in their respective domains. As  $r'$  and  $m$  uniquely identify  $s'$ ,  $(r', s', m)$  is a random triplet and independent of the signer's view.

No apparent security weakness of this protocol is known. Some security proofs of this protocol have been discussed in [8.19, 8.30]. Particularly, [8.30] shows that the view of the signer in the protocol and the signature are statistically independent, i.e., generated signatures are witness-indistinguishable.

### 8.5.2 The Digital Cash Scheme

In this section, we take a look at a previously proposed digital-cash scheme, which is based on the blind Nyberg–Rueppel digital-signature scheme. [8.28]

**The setup protocol.** On inputting a security parameter  $k$ , the bank B runs a key generation algorithm to generate:

- a large prime  $p$  and a large number  $q$  such that  $q|p - 1$ ,
- three generators  $g, g_1$  and  $g_2$  of the unique subgroup  $\mathbb{G}_q$  of the multiplicative group  $\mathbb{Z}_p^*$ ,
- a randomly chosen collision-intractable hash function  $\mathcal{H}(\cdot)$  of polynomial size of  $k$  that maps its inputs to  $\mathbb{Z}_q$ ,
- a random number  $x \in \mathbb{Z}_q$  and
- $h_1 = g_1^x$  and  $h_2 = g_2^x$ .



B has now the secret key  $x$  and the public tuple  $(p, q, g_1, g_2, h, h_1, h_2, \mathcal{H}(\cdot))$  respectively.

**The account setup.** The setup phase is similar to those we studied previously in this chapter. To set up an account at B, C chooses  $U \neq 0 \in_R \mathbb{G}_q$  at random and calculates  $I = g_1^U$ . B regards  $I \neq 1$  as C's account identification and sends  $z = (Ig_2)^x$  to C. Note that  $I$  is the unique link to the user's real name, while  $U$  is unknown to the bank.  $U$  can be computed by the bank only when the user double spends a coin.

**The withdrawal protocol.** The withdrawal protocol between C and B is given in Fig. 8.7.

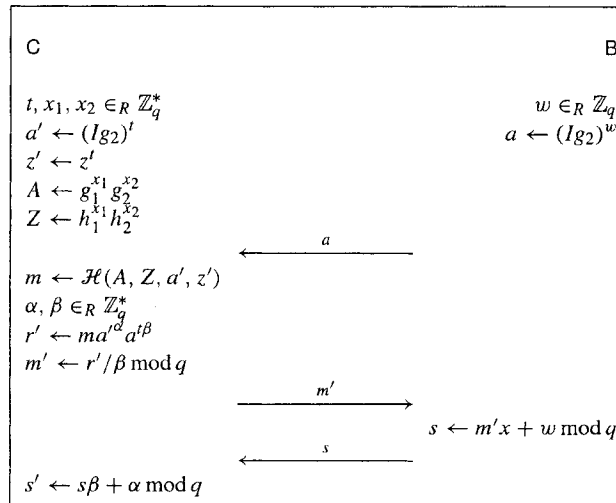


Fig. 8.7 The withdrawal protocol

The blind Nyberg–Rueppel signature scheme is essential for the anonymity of clients. Note that the base used in the protocol is not the fixed base  $g$  of the signer public key, but the base  $(Ig_2)^i$  for a random number  $i$  chosen by the user. At the end of the withdrawal protocol, the client should receive the blind Nyberg–Rueppel signature  $\text{Sign}(A, Z) = (A, Z, z', a', r', s')$ , which is verified using the equation

$$\mathcal{H}(A, Z, a', z') = a'^{-s'} z'^{r'} r'.$$

It is important to verify that the secret key used in the signature generation is the secret key  $x$  of the bank. Otherwise, the user can create such a signature using any secret key. This verification is described in the payment protocol.

**The payment protocol.** The payment protocol is run between C and V. The payment of a coin  $(A, Z, z', a', r', s')$  is described in Fig. 8.8. As for the proof of equality of

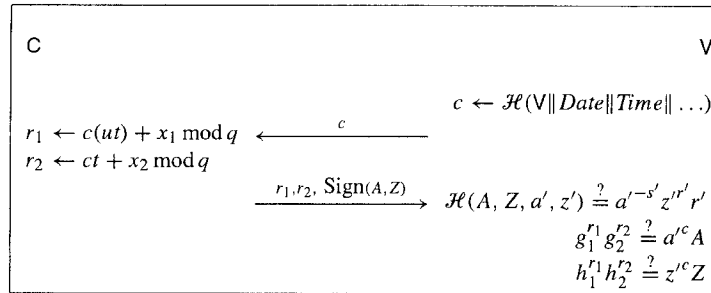


Fig. 8.8 The payment protocol

discrete logarithms, for a random challenge  $c$  if

$$g_1^{r_1} g_2^{r_2} \stackrel{?}{=} a'^c A,$$

$$h_1^{r_1} h_2^{r_2} \stackrel{?}{=} z'^c Z,$$

we must have  $\log_{a'} z' = \log_{g_1} h_1$ . This shows that the bank's secret key  $x = \log_{g_1} h_1$  was used in the generation of  $\text{Sign}(A, Z)$ .

**The deposit protocol.** V can deposit the coin  $\text{Sign}(A, Z)$  at any suitable time. The deposit procedure is to send the transcript of the payment to B. B verifies the payment procedure and accepts the coin if V follows the procedure correctly and the coin satisfies all verifications as checked in the payment phase.

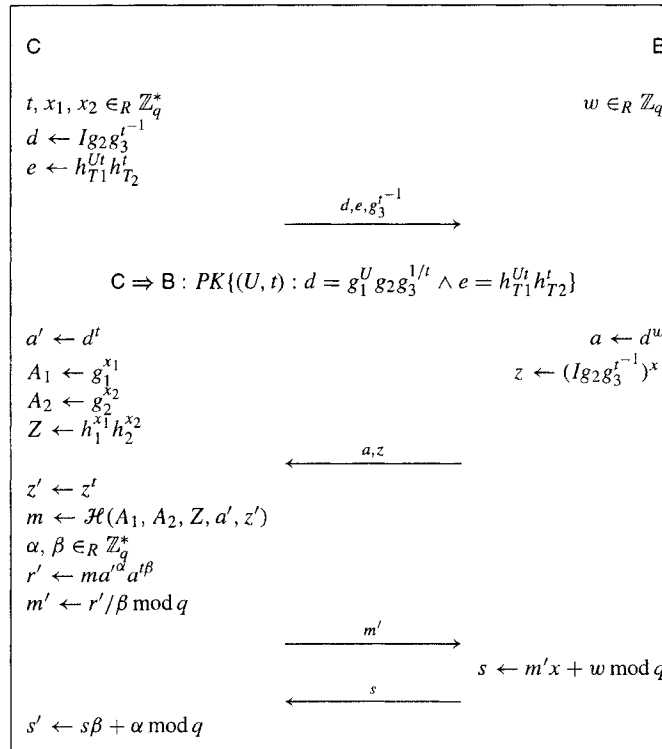
### 8.5.3 The Fair-Digital-Cash Scheme

We now convert the digital-cash scheme described previously in this section into a fair version.

**The setup.** The setup phase is similar to the original scheme. Here, we give only the difference. Let  $x \in \mathbb{Z}_q$  be the secret key of B. The public data of B consists of tuple:  $(p, q, g_1, g_2, g_3, h_1 = g_1^x, h_2 = g_2^x)$ , where  $(g_1, g_2, g_3) \in (\mathbb{Z}_p^*)^3$ . To set up an account at B, C chooses  $U \neq 0 \in_R \mathbb{G}_q$  at random and calculates  $I = g_1^U$ . B regards  $I \neq 1$  as C's account identification and sends  $z = (I g_2 g_3)^x$  to C.

The trusted authority T's secret key is  $\tau \in \mathbb{Z}_q$  and his public key is the doublet  $(h_{T1} = g_1^\tau, h_{T2} = g_2^\tau)$ .

**The withdrawal protocol.** The withdrawal protocol is executed between C and B. Formally, the protocol is given in Fig. 8.9.



**Fig. 8.9** The withdrawal protocol

The withdrawal protocol is basically the blind Nyberg–Rueppel digital signature scheme but the base is  $d^t = (Ig_2)^t g_3$ . At the end of the withdrawal protocol, the user should receive the blind Nyberg–Rueppel signature

$$\text{Sign}(A_1, A_2, Z) = (A_1, A_2, Z, z', a', r', s')$$

which is verified using the equation

$$\mathcal{H}(A_1, A_2, Z, a', z') = a'^{-s'} z'^{r'} r'$$

Besides  $(A_1, A_2, Z, z', a', r', s')$ , the bank also stores the value  $e$ , given below, in the coin database for referencing.

In this protocol, the value  $A$  is split into two values  $A_1$  and  $A_2$ . This is necessary to achieve owner tracing. The extra computation of  $(d, e)$  and the associate proof of



The completeness of the scheme is straightforward. As the scheme is developed using our proposed anonymous-digital-cash scheme, it is easy to show that this fair-digital-cash scheme satisfies all security requirements of the anonymous e-cash scheme, e.g., unforgeability. It remains to show that user tracing and coin tracing can be satisfied.

**Anonymity revocation.** There are two possible anonymity controls in this scheme. One is to identify the user in a payment transaction and the other is to identify the history, i.e., the life cycle of a coin. The former is referred to as user tracing and the latter is referred to as coin tracing. In practice, T should only run these protocols under a court order. Formally, the user-tracing and coin-tracing protocols work as follows:

### Client Tracing

To identify the client in a payment transaction, B brings  $(D_1, D_2)$  to T who then computes

$$D_1/D_2^\tau = g^U h_{T_1}^\rho / g_1^{\tau\rho} = g^U,$$

which identifies the client.

The soundness of this protocol is due to the proof of knowledge

$$\text{PK}\{(U, t, \rho) : a_1 = g_1^{Ut} \wedge a_2 = g_2^t \wedge D_1 = g^U h_{T_1}^\rho \wedge D_2 = g_1^{\rho}\},$$

which shows  $g^U$  is the plaintext corresponding to the ElGamal ciphertext  $(D_1, D_2)$  encrypted using T's public key for the client secret information  $U$ . In the client-tracing protocol, T simply decrypts the ciphertext and returns  $g^U$  which identifies the client.

Note that this procedure is not possible for other parties as only T can decrypt a ciphertext encrypted using T's public key.

### Coin Tracing

Identifying a coin history can be done in two different ways. One is to identify the coin payment for a given coin withdrawal and the other is to identify the coin withdrawal for a given coin payment.

In the later case, B sends to T the payment transcript. Then T computes the value

$$d'/g_3^\tau = ((I g_2)^t)^\tau = g_1^{U\tau} g_2^{t\tau} = h_{T_1}^{ut} h_{T_2}^t = e,$$

and sends the value  $e$  back to B. The anonymity revocation is done by searching for the computed value  $e$  in the coin withdrawal reference database.

In the former case, B sends to T the withdrawal reference  $e$ . Then T computes and sends to B the value

$$e^{1/\tau} g_3 = h_{T1}^{U/\tau} h_{T2}^{t/\tau} g_3 = g_1^{U_t} g_2^{t} g_3 = a'.$$

Now, the anonymity revocation is done by matching this computed value  $a'$  with the value  $a'$  in every deposited coin.

## 8.6 Summary

There are various digital-cash protocols having been proposed in past two decades. We can refer them to as three forms: normal digital-cash (e.g., [8.1, 8.2]), divisible digital-cash [8.7], and fair digital-cash (e.g., [8.14]). In this chapter, we have described three typical digital-cash schemes: the digital-cash scheme proposed by Brands[8.2], and the digital-cash and the fair digital-cash scheme proposed by Nguyen et. al. [8.14] We hope that these schemes give the reader an overall picture of digital-cash.

## 8.7 Appendix

This section gives protocols for proving the knowledge of various discrete logarithms. Some of these protocols presented in this section are borrowed from Camenisch [8.17], which gives a rigorous treatment of proofs of knowledge about discrete logarithms. The interactive versions of these protocols are known to be witness-indistinguishable and proofs of knowledge. The reader is also referred to [8.15, 8.18, 8.26, 8.29] for detailed discussions of these protocols and other variations.

In the following, we assume that  $g, h_1, h_2, g_1, \dots, g_m \in \mathbb{G}_q (\subset \mathbb{Z}_p^*)$  are generators of order  $q$  such that computing a representation of any generator with respect to other generators is infeasible.

**Proving the Knowledge of Discrete Logarithms.** A proof of knowledge of the discrete logarithm proves the knowledge of the secret number  $x \in \mathbb{Z}_q$  from  $y = g^x$ . This proof is actually part of the Schnorr identification scheme. Following the notations of [8.17, 8.18], we denote this protocol as

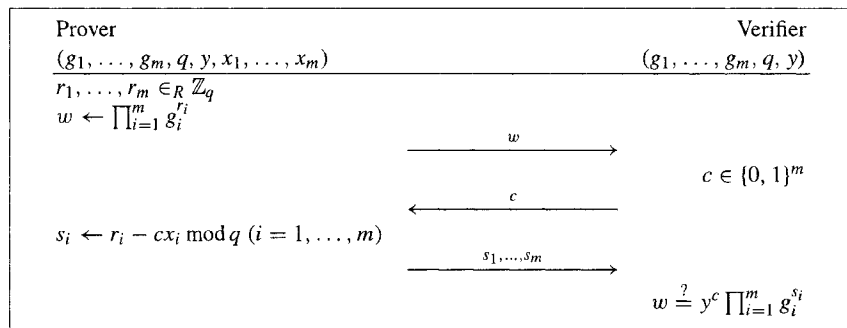
$$\text{PK}\{(\alpha) : y = g^\alpha\}.$$

The proof is straightforward. We omit it here.

**Proving the knowledge of a Representation.** The proof of knowledge of a representation proves the knowledge of a representation of  $y$  to the bases  $g_1, \dots, g_m$ , which is denoted by

$$\text{PK}\{(x_1, \dots, x_m) : y = \prod_{i=1}^m g_i^{x_i}\}.$$

This proof is first introduced in [8.22] and is given in Fig. 8.11.



**Fig. 8.11** A proof of representation of  $y$  to the bases  $g_1, \dots, g_m$

The correctness of this protocol is due to

$$y^c \prod_{i=1}^m g_i^{s_i} = \prod_{i=1}^m g_i^{cx_i} \prod_{i=1}^m g_i^{s_i} = \prod_{i=1}^m g_i^{cx_i + s_i} = \prod_{i=1}^m g_i^{r_i} = w.$$

The soundness is due to the fact that given a same value  $w$ , if the prover can answer two different challenges  $c$  and  $c'$  correctly, the knowledge extractor obtains two sets of  $(c, s_1, \dots, s_m)$  and  $(c', s'_1, \dots, s'_m)$  and extract the secret  $x_i$  as:

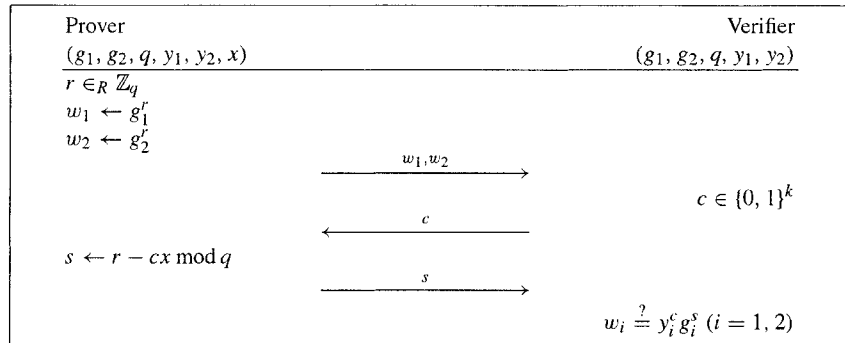
$$x_i = \frac{s_i - s'_i}{c' - c} \pmod q.$$

The zero-knowledge holds because a honest verifier can construct a valid view by choosing  $s_1, \dots, s_m$  and  $c$  at random and computing  $w = y^c \prod_{i=1}^m g_i^{s_i}$ .

**Proving the Equality of Discrete Logarithms.** This proof proves not only the knowledge of secret keys but also certain relations among them. In the most simplest form, it is a proof of knowledge and of equality of discrete logarithm of  $y_1$  to the base  $g_1$  and  $y_2$  to the base  $g_2$ . This proof was first introduced by Chaum and Pedersen in [8.23]. Let us denote this protocol by:

$$\text{PK}\{(\alpha) : y_1 = g_1^\alpha \wedge y_2 = g_2^\alpha\}.$$

The intuition is to run the proof of knowledge of discrete logarithm of  $y_1$  to the base  $g_1$  and of discrete logarithm of  $y_2$  to the base  $g_2$ , and then  $\log_{g_1} y_1 = \log_{g_2} y_2$  only if the prover can return the same answer in both cases for a random challenge chosen by the verifier. Formally, this protocol is given in Fig. 8.12.

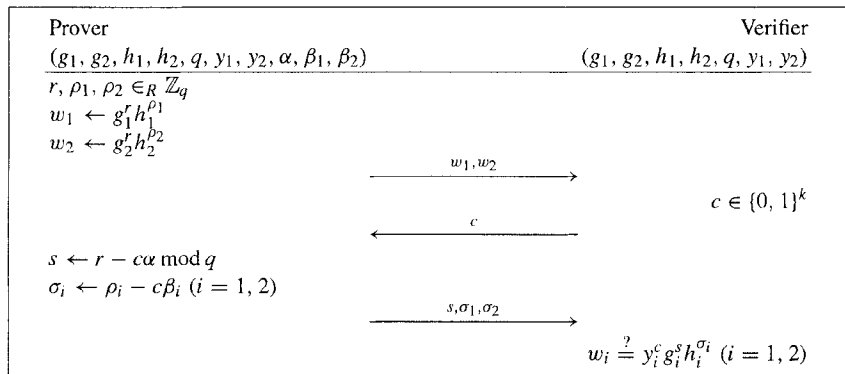


**Fig. 8.12** The proof of  $\log_{g_1}(y_1) \equiv \log_{g_2}(y_2)$

It is trivial to extend the proof system of equality of discrete logarithms to a proof system of equality of representations. One of such proof is the proof of knowledge of representation of  $y_1$  and  $y_2$  to the bases  $(g_1, h_1)$  and  $(g_2, h_2)$ , respectively and that the representation of  $y_1$  to  $g_1$  and  $y_2$  to  $g_2$  are equal. This protocol, which is denoted by

$$PK\{(\alpha, \beta_1, \beta_2) : y_1 = g_1^\alpha h_1^{\beta_1} \wedge y_2 = g_2^\alpha h_2^{\beta_2}\},$$

is described in Fig. 8.13. This proof introduced in [8.23] is the basic building block for many blind digital signatures and anonymous-digital-cash schemes.



**Fig. 8.13** The proof of equality of representations

**Proving knowledge of inverse of discrete logarithms.** In this protocol, we give the proof for: given  $y_1 = g_1^t$  and  $y_2 = g_2^{t^{-1}}$ , Proving that  $(\log_{g_1} y_1)^{-1} = \log_{g_2} y_2$ . The protocol is given in Figure 8.14.