US005768385A

United States Patent [19]

Simon

[11] Patent Number: 5,768,385

[45] Date of Patent: Jun. 16, 1998

[54] **UNTRACEABLE ELECTRONIC CASH**

[75] Inventor: **Daniel R. Simon**, Redmond, Wash.

[73] Assignee: **Microsoft Corporation**, Redmond, Wash.

[21] Appl. No.: **521,124**

[22] Filed: **Aug. 29, 1995**

[51] **Int. Cl.**[6] **H04L 9/00**; H04L 9/30

[52] **U.S. Cl.** **380/24**; 380/23; 380/25; 380/30; 380/49

[58] **Field of Search** 380/23, 24, 25, 380/29, 30, 49, 59, 4, 9, 50

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,914,698	4/1990	Chaum	380/30
4,947,430	8/1990	Chaum	380/25
4,949,380	8/1990	Chaum	380/30
4,987,593	1/1991	Chaum	380/30 X
4,991,210	2/1991	Chaum	380/30
4,996,711	2/1991	Chaum	390/30
5,131,039	7/1992	Chaum	380/23
5,276,736	1/1994	Chaum	380/24
5,373,558	12/1994	Chaum	380/23

OTHER PUBLICATIONS

A. Pfitzmann, "How to Implement ISDNs Without User Observability—Some Remarks," TR 14/85, Fakultät für Informatik Universität Karlsruhe, 1985.

Okamoto, et al., "Universal Electronic Cash," Proc. CRYPTO 191, Springer–Verlag (1992), pp. 324–337.

Rompel, "One–Way Functions Are Necessary and Sufficient for Secure Signatures," Proc. 31st IEEE Symp. on Foundations of Computer Science (1990), pp. 387–394.

Brands, "Untraceable Off–line Cash in Wallet with Observers" Proc. CRYPTO '93, Springer–Velag (1994) pp. 302–318.

Yacobi, "Efficient Electronic Money," Proc. ASIACRYPT 194, Springer–Verlag (1994).

Rackoff, et al. "Cryptographic Defense Against Traffic Analysis," Proc. 25th ACM Symp. on the Theory of Computation (1993).

Chaum, "Online Cash Checks," Proc. EUROCRYPT '89, Springer–Verlag (1989), pp. 288–293.

Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," Journal of Cryptology, vol. 1, No. 1 (1988), pp. 65–75.

Chaum, "Privacy Protected Payments—Unconditional Payer and/or Payee Untraceability," Smart Card 2000: The Future of IC Cards—Proc. IFIP WG 11.6 Int'l Conf. North–Holland (1989) pp. 69–93.

Pfitzmann, et al. "ISDN–MIXes—Untraceable Communication with Very Small Brandwidth Overhead," Proc. Kommunikation in verteilten Systemen (1991), pp. 451–463.

Even, et al. "Electronic Wallet," Proc. CRYPTO '83, Plenum Press (1984), pp. 383–386.

Chaum, et al. "Untraceable Electronic Cash," Proc. CRYPTO '88, Springerverlag (1990), pp. 319–327.

Franklin, et al., "Secure and Efficient Off–Line Digital Money," Proc. 20th Int'l Colloquim on Automata Languages and Programming, Springer–Verlag (1993), pp. 265–276.

Chaum, "Achieving Electronic Privacy," Scientific American, vol. 267, No. 2 (1992), pp. 96–101.

Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," CACM, vol. 24, No. 2 (1981) pp. 84–88.

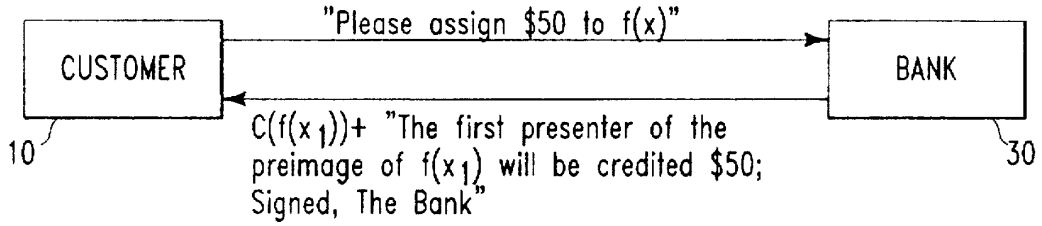
Primary Examiner—Bernarr E. Gregory

Attorney, Agent, or Firm—Michaelson & Wallace; Peter L. Michaelson

[57] **ABSTRACT**

An electronic cash protocol including the steps of using a one-way function $f_1(x)$ to generate an image $f_1(x_1)$ from a preimage x_1; sending the image $f_1(x_1)$ in an unblinded form to a second party; and receiving from the second party a note including a digital signature, wherein the note represents a commitment by the second party to credit a predetermined amount of money to a first presenter of the preimage x_1 to the second party.

30 Claims, 2 Drawing Sheets



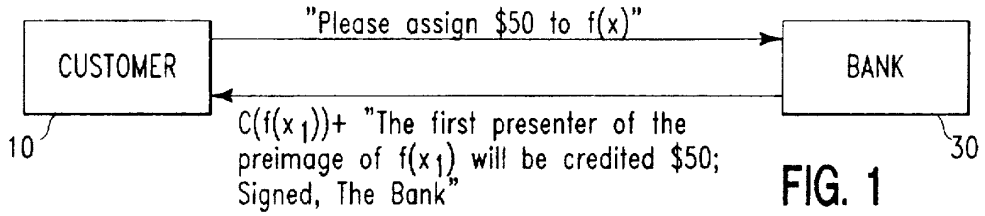


FIG. 1

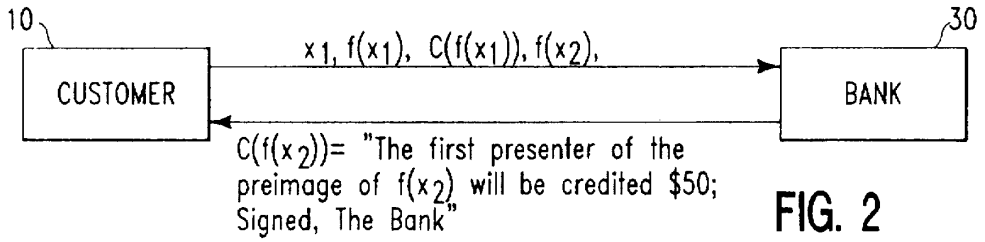


FIG. 2

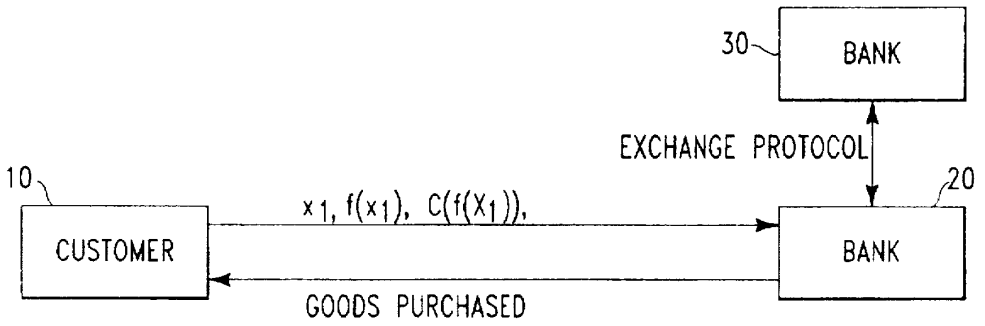


FIG. 3

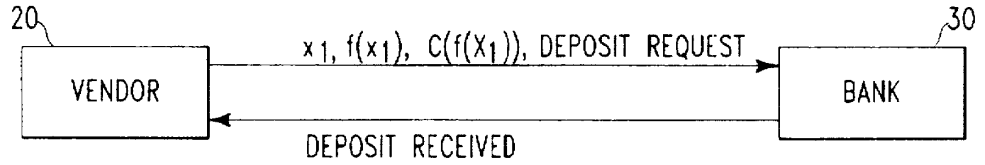


FIG. 4

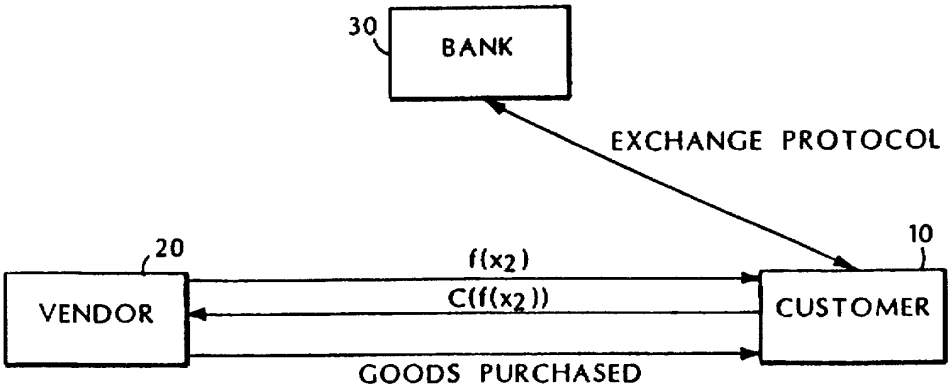


FIG. 5

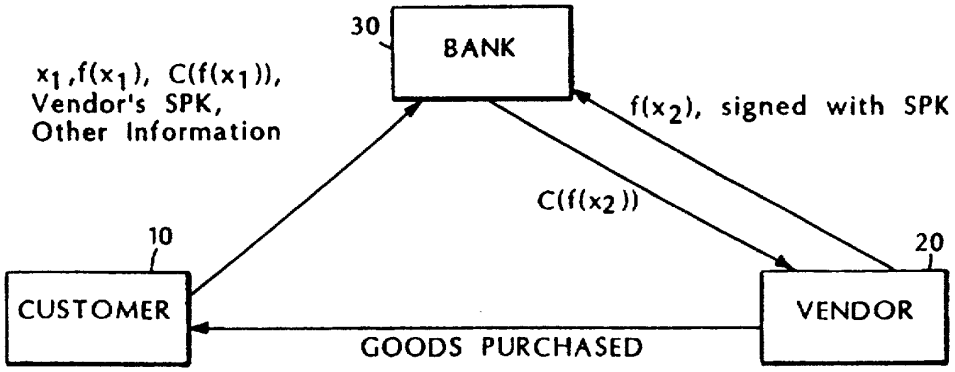


FIG. 6

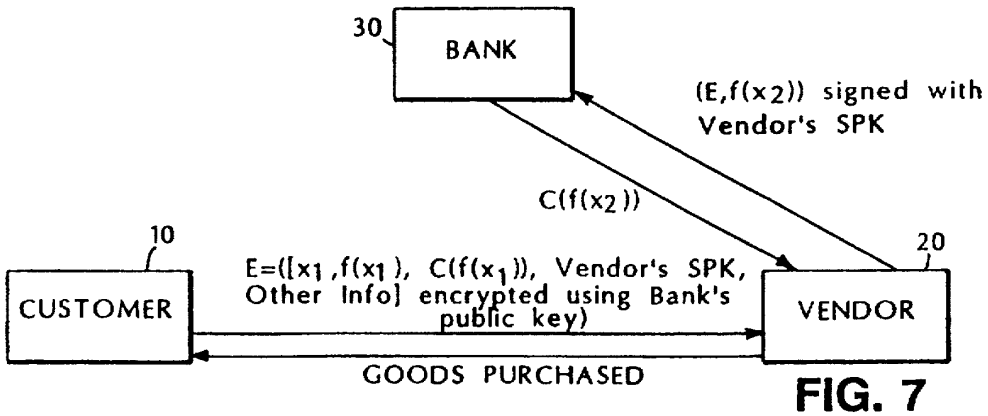


FIG. 7

UNTRACEABLE ELECTRONIC CASH

BACKGROUND OF THE INVENTION

The invention generally relates to electronic cash systems.

The ultimate intuitive goal of an electronic cash system is to combine the best features of physical cash (privacy, anonymity, unforgeability) with the best features of electronic commerce (speed, ease and potential security of transport and storage). The fundamental difficulty with attempting to implement anonymous electronic cash, however, is simple to state: if the possessor of an electronic "coin" is not identified in two successive transactions, then how is he or she to be prevented from acting as if the first transaction never occurred, and spending the same coin again. The first proposed solution to this problem was presented by Chaum, Fiat and Naor (see D. Chaum, A Fiat and M. Naor, Untraceable Electronic Cash, Proc. CRYPTO '88, Springer-Verlag (1990), pp. 319–327.), and was based on the premise that it would be sufficient for such "double spending" to be detected, and the spender identified, upon presentation of the same "electronic coin" twice to the central bank. This premise has also been used in a number of other proposed solution, all with the advantage that the bank need not be involved in each transaction. Practically speaking, however, this premise has enormous drawbacks. Fraudulent transactions are detected only long after they have taken place, and if the perpetrator can be confident of not being brought to justice (either by being inaccessible or by managing to use someone else's identity and cash), then he or she can double-spend at will.

However, if such fraudulent use of electronic cash is to be prevented, then some authority must somehow be involved in each transaction as it occurs, so as to be able to recognize and alert targets of double-spending. How, then, is anonymity to be preserved. One approach is to rely on tamper-resistant hardware to force spenders to behave "honestly" (ie., not to double-spend) (see, for example, S. Even, O. Goldreich and Y. Yacobi, Electronic Wallet, Proc. CRYPTO '83, Plenum Press (1984), pp. 383–386.). Schemes based on this premise are, however, extremely "brittle". If anyone ever succeeds in tampering with the hardware, then not only is that person capable of double-spending, but anyone, anywhere who obtains (e.g. purchases, perhaps) the information hidden in the hardware can spend arbitrarily high amounts at will. Current tamper resistance technology is far from being dependable enough to be trusted to thwart such an enormous risk.

Another approach is cryptographic. For example, under certain very strong cryptographic assumptions, it is possible to construct protocols that create "blinded" cash—information which can be recognized later as valid cash, but cannot be connected with any particular run of the protocol. (See, for example, D. Chaum, Privacy Protected Payments—Unconditional Payer and/or Payee Untraceability, SMART CARD 2000: The Future of IC Cards—Proc. IFIP WG 11.6 Int'l Conf., North-Holland (1989), pp. 69–93; and D. Chaum, Online Cash Checks, Proc. EUROCRYPT '89, Springer-Verlag (1989), pp. 288–293.)

SUMMARY OF THE INVENTION

We present a simple, practical online electronic cash system based on the assumption of a network in which anonymous, untraceable communication is possible. In general, the invention uses two simple primitives, namely a one-way function and a signature scheme. These are both well known in the art; and descriptions can be found in publicly available literature on cryptography, e.g. Applied Cryptography, Bruce Schneier, John Wiley & Sons, Inc. (1994). The anonymity of spenders as well as guaranteeing their electronic coins' validity, but also the coins used are unforgeable and cannot be spent more than once.

In general, in one aspect, the invention is an electronic cash protocol including the steps of using a one-way function $f_1(x)$ to generate an image $f_1(x_1)$ from a preimage x_1; sending the image $f_1(x_1)$ in an unblinded form to a second party; and receiving from the second party a note including a digital signature. The received signed note represents a commitment by the second party to credit a predetermined amount of money to a first presenter of the preimage x_1 to the second party.

Preferred embodiments include the following features. The electronic cash protocol also includes sending the preimage x_1 to a third party as payment for purchase of goods or services from the third party. Alternatively, it further includes selecting a second preimage x_2; using a second one-way function $f_2(x)$ to generate a second image $f_2(x_2)$ from the second preimage x_2; sending the first preimage x_1 and the unblinded form of the second image $f_2(x_2)$ to the second party; and receiving from the second party a note including a digital signature, the note representing a commitment by the second party to credit the predetermined amount of money to a first presenter of the second preimage x_2 to the second party. In both cases, $f_1(x)$ and $f_2(x)$ are the same function. In the latter case, the sending of the first preimage x_1 and the unblinded form of the second image $f_2(x_2)$ to the second party is performed anonymously and the second party is a bank.

Also in preferred embodiments, the protocol includes the steps of concatenating a signature key of a third party with the first preimage x_1 to form a block of information; encrypting the block of information by using an encryption key of the second party to generate an encrypted block of information; and sending the encrypted block of information to the third party.

In general, in another aspect, the invention is an electronic cash protocol including the steps of receiving a first preimage x_1 from a first party, wherein the preimage x_1 produces a first image $f_1(x_1)$ when processed by a first one-way function $f_1(x)$ and there being associated with said first preimage x_1 a commitment by a second party to credit a predetermined amount ofmoney to a first presenter to the second party of said first preimage x_1; selecting a second preimage x_2 ; using a second one-way function $f_2(x)$ to generate a second image $f_2(x_2)$ from the second preimage x_2; sending the first preimage x_1 and an unblinded form of the second image $f_2(x_2)$ to the second party; and receiving from the second party a note including a digital signature, wherein the note represents a commitment by the second party to credit the predetermined amount of money to a first presenter of the second preimage x_2 to the second party.

In general, in yet another aspect, the invention is an electronic cash protocol including the steps of receiving from a first party an encrypted block of information, wherein the block of encrypted information was generated by first concatenating a public signature key of a second party with a first preimage x_1 to form a block of information and then encrypting the block of information by using an encryption key of a third party; selecting a second preimage x_2; using a second one-way function $f_2(x)$ to generate an image $f(x_2)$ from the preimage x_2; forming a message including the encrypted block of information along with the image $f(x_2)$ in

an unblinded form; sending the message to the third party; and receiving from the third party a signed note including a digital signature, wherein the note represents a commitment by the third party to credit a predetermined amount of money to a first presenter of the preimage x_2 to the third party.

In general, in still another aspect, the invention is an electronic cash protocol including the steps of receiving from a first entity an unblinded form of an image $f_1(x_1)$ that was generated by applying a one-way function $f_1(x)$ to a preimage x_1; generating a message which contains a commitment to credit a predetermined amount of money to a first presenter of the preimage x_1; signing the message with a digital signature; and sending the message along with the digital signature to the first party.

In preferred embodiments, the electronic cash protocol also includes subsequently receiving the preimage x_1 from a third party; checking a database for the preimage x_1; if the preimage x_1 is not found in the database, crediting the third party with the predetermined amount of money; and adding the preimage x_1 to the database. Alternatively, the protocol includes subsequently receiving the preimage x_1 and an unblinded image $f_2(x_2)$ from a third party, wherein the unblinded image $f_2(x_2)$ was generated by applying a one-way function $f_2(x)$ to a preimage x_2; checking a database for the preimage x_1; if the preimage x_1 is not found in the database, generating a signed note including a digital signature, wherein the note represents a commitment to credit the predetermined amount of money to a first presenter of the preimage x_2; and adding the preimage x_1 to the database.

Also in preferred embodiments, the invention features receiving a message from a second party, wherein the message was generated by concatenating an encryption key of a third party with a first preimage x_1 to form a block of information, by encrypting the block of information by using a first encryption key to generate an encrypted first block, and by concatenating an unblinded image $f_2(x_2)$ to the encrypted first block of information, wherein the unblinded image $f_2(x_2)$ was generated by using a one-way function $f_2(x)$ to generate an image $f_2(x_2)$ from a preimage x_2. It further features decrypting the encrypted first block of information; generating a note including a digital signature, wherein the note represents a commitment to credit a predetermined amount of money to a first presenter of the preimage x_2; and sending the note to the second party.

In general, in yet another aspect, the invention is an electronic cash protocol including the steps of sending an unblinded image $f_2(x_2)$ to a second party, wherein the unblinded image $f_2(x_2)$ was generated by applying a one-way function $f_2(x)$ to a preimage x_2; receiving a signed note from the second party, wherein the unblinded note includes a digital signature and represents a commitment to credit the predetermined amount of money to a first presenter of the preimage x_2; and in response to receiving the unblinded note from the second party, authorizing the delivery of goods and/or services to a third party.

The invention offers a simple, inexpensive way of doing cash-like transactions where the item of exchange (i.e., the withdrawn coin) has the properties of actual cash. For example, it is: (1) more or less anonymous; (2) secure; (3) inexpensive to use; and (4) easy to carry around and exchange.

Parties are protected against a dishonest bank's reneging on withdrawn coins by the fact that they keep secret the value x_1 for a particular coin until it is spent. As long as a particular coin $f(x_1)$ is deposited publicly and non-anonymously, the bank can be required to honor it unless it can supply the associated x_1. Of course, the bank can renege on an anonymously exchanged coin $f(x_1)$ during the actual exchange, by claiming upon receiving x_1 that the coin has already been spent. However, the bank cannot possibly know who is being cheated by such a "dine and dash" ploy, and is therefore vulnerable to monitoring and public exposure.

Finally, banks themselves are protected against counterfeiting by the security of the digital signature scheme used to sign electronic coins. Moreover, they are protected against "double-spending" (or "double deposit") by their ability to store x_1 values for coins in perpetuity.

Other advantages and features will become apparent from the following description of the preferred embodiment and from the claims.

BRIEF DESCRIPTION OF THE DRAWING

FIG. **1** is a diagram of a non-anonymous withdrawal protocol;

FIG. **2** is a diagram of an anonymous exchange protocol;

FIG. **3** is a diagram of an anonymous purchase protocol;

FIG. **4** is a diagram of a non-anonymous deposit protocol;

FIG. **5** is a diagram of an anonymous alternate payment protocol;

FIG. **6** is a diagram of an anonymous or non-anonymous "drop" payment or money order protocol; and

FIG. **7** is a diagram of an encrypted money order protocol.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The ability to communicate anonymously is in some sense necessary a priori if anonymous cash transactions are to occur, since information about a party's communications will obviously reveal information about the party's business dealings. In practice, the anonymity of communication may be based on nothing more than confidence that the telephone company safeguards the confidentiality of its system. Alternatively, parties may place trust in one or more "anonymous remailers" to obscure identities of the parties , or rely on an implementation of one of the other techniques from the publicly available literature.

Suppose, not only that communications between parties are anonymous with respect to third parties, but also that the communicating parties are anonymous to each other. (In typical implementations, the latter condition is a natural consequence of the former, barring self-identification.) A simple, somewhat anonymous electronic cash protocol in such a setting is shown in FIG. **1**.

In the following descriptions of various protocols (see FIGS. 1–7), we generally refer to three parties, namely, a Customer **10**, a Vendor **20**, and a Bank **30**. Customer **10** is of course generally representative of the payor and Vendor **20** is generally representative of the payee. It should be understood, however, that these designations are chosen for purposes of clarity and that they are not meant to limit the scope of the invention. It would be just as valid to have referred to them as Party A, Party B and Party C.

In the figures, the different entities are represented by blocks and the transfers of information from one entity to another are indicated by lines interconnecting the appropriate blocks. Each line represents a transfer of certain information from one entity to another in the direction indicated by an arrow at the end of the line. The information that is transferred is summarized symbolically below the lines.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.