IMES DISCUSSION PAPER SERIES

An Electronic Money Scheme

- A Proposal for a New Electronic Money Scheme which is both Secure and Convenient -

Yasushi Nakayama, Hidemi Moribatake,
Masayuki Abe, Eichiro Fujisaki

Discussion Paper No. 97-E-4

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

C.P.O BOX 203 TOKYO
100-91 JAPAN

NOTE: IMES Discussion Paper Series is circulated in order to stimulate discussion and comments. Views expressed in Discussion Paper Series are those of authors and do not necessarily reflect those of the Bank of Japan or the Institute for Monetary and Economic Studies.

IMES Discussion Paper Series 97-E-4
June 1997

An Electronic Money Scheme

- A Proposal for a New Electronic Money Scheme which is both Secure and Convenient -

Yasushi Nakayama *, Hidemi Moribatake **,
Masayuki Abe **, Eichiro Fujisaki **

Abstract

As the Internet expands, a variety of trials for realizing electronic payment systems have been made in many countries. In particular, electronic money, which employs electronic data embodying monetary value exchangeable through open networks, has been extensively researched and experimented. It is regarded as the infrastructural technology for the realization of electronic commerce.

This paper discusses the requirements to be met for electronic money to become a new secure low-cost monetary service, i.e. security, unique convenience, and inheritance of merits from cash. We then propose a basic design of a new electronic money scheme which fulfills these requirements and present the outline of the protocol of this new electronic money system which includes some new ideas.

Key words: electronic money, electronic cash, issuing institution, privacy, direct transferability between individuals, blind signature, tamper resistance

JEL classification: E49

* Research Division 2, Institute for Monetary and Economic Studies, Bank of Japan (E-mail: nakayama@imes.boj.go.jp)
** Information and Communication Systems Laboratories, Nippon Telegraph and Telephone Corporation (E-mail: hidemi@sucaba.isl.ntt.co.jp, abe@isl.ntt.co.jp, fujisaki@sucaba.isl.ntt.co.jp)

The authors would like to thank Associate Professor Tsutomu Matsumoto (Yokohama National University) for helpful comments.

An Electronic Money Scheme

- A Proposal for a New Electronic Money Scheme
which is both Secure and Convenient -

1. Introduction

As the Internet expands, a variety of trials for realizing electronic payment systems have been made in many countries. In particular, electronic money, which employs electronic data embodying monetary value exchangeable through open networks, has been extensively researched and experimented. It is regarded as the infrastructural technology for the realization of electronic commerce.

This paper discusses the requirements to be met for electronic money to become a new secure low-cost monetary service. We propose a new electronic money scheme which achieves high technical quality: a common electronic money scheme in which a number of banks can participate, compatibility of anonymity and traceability of invalid use, divisibility, and transferability between individuals.

2. Requirement

Currently, various methods of payment are proposed with the aim of realizing electronic commerce, i.e. electronic money (in a narrow sense), electronic methods for credit card payment, electronic checks, and on-line banking. With the exception of electronic money, these methods can be considered to be ones that provide consumers with a new access channel to conventional payment or banking services, such as credit card services or electronic funds transfers, utilizing computer networks such as the Internet or other telecommunications networks. Electronic money, by contrast, is proposed under the concept that the data are money, and those themselves contain value, and has drawn much attention recently. Although some electronic money projects have proceeded to the stage of a field test or limited practical usage, many experts say that much more improvement, i.e. upgrading the level of security and of convenience for users, is needed before full-fledged implementation.

This chapter describes the requirements to be met for electronic money to be accepted widely in society. They are : (1) security, (2) unique convenience, and (3) inheritance of merits from cash.

(1) Security

For electronic money to be secure, invalid use by alteration, forgery, or duplication must be almost impossible. In order for electronic money to become widely accepted as a

medium for transaction settlements, its security must be trusted by society. To this end, multiple security measures from multiple viewpoints are essential, so that even if, by any chance, one of these security measures were compromised, the other security measures could still thwart illegal actions.

An example of combining security measures is minimizing the possibility of illegal actions (pre measure) and provision of method for tracing the suspect if an illegal action has occurred (post measure).

(2) Unique convenience

Electronic money has the possibility of providing a higher level of convenience than cash. This convenience is considered to be the primary incentive for society to accept its wide use. For example, it is possible to design an electronic money scheme, in which electronic money can be used not only in ordinary stores like cash, but also over open networks such as the Internet, providing a new medium of payment for electronic commerce, which is expected to increase in the future. It is also possible to design a scheme in which no change is needed for payment, because division into any amount is made possible to make exact payment (divisibility).

(3) Inheritance of merits from cash

For the wide use of electronic money, it is important to design it so that it continues the merits of cash, many of which are unique as compared with other payment instruments. One of the major characteristics of cash is that anyone, regardless of credit history, can use and accept it. This is because cash itself contains value, and therefore there is no need to check the counterparty's credibility. Cash payment can be made final by mutual consent of the payer and the payee without an intermediary (off-line transaction), and therefore it can be used anywhere for any reason and can be transferred directly to other individuals (transferability), for example from consumer to consumer. In addition, cash is treated exactly the same regardless of which bank it has been withdrawn from (equal treatment by all banks).

Another characteristic of cash is the protection of the users' privacy. Anonymous transactions can be realized by means of cash, leaving no purchase history. The level of privacy provided by an electronic money system can be classified into two categories.

The first category ensures that the user’s privacy could not be violated even if the store and the bank (the electronic money issuer and the settlement service provider) were to collude

(untraceability). The second category ensures, in addition to the first, that no connection can be made between the information on the use of electronic money by the same person on different occasion (unlinkability).

The requirements for electronic money can be summarized as follows.

(1) Security

(a) Preventing invalid use (illegal acts such as forgery or copying are impossible)

(b) Identifying malicious users (traceability of suspects when illegal acts occur)

(2) Unique convenience of electronic money

(c) Divisibility (enables users to divide the electronic money into desired denominations)

(d) Over-the-counter and over-a-network payment capability (because the value consists of information only, payment not only over the counter but also over a network is possible)

(e) Efficient management of issuance and administration (issuance and administration of electronic money are conducted efficiently, providing high-speed processing at low cost)

(3) Inheritance of merits from cash

(f) Privacy protection

(f-1) Untraceability (even if the store and the bank collude, it is impossible for them to uncover the user's purchase history)

(f-2) Unlinkability (no connection can be made between the information on the use of electronic money by the same person on different occasions)

(g) Off-line operability (the payment process can be completed without third party intervention)

(h) Direct transferability between individuals (received electronic money can be directly transferred to other individuals)

(i) Portability (electronic money can be used through a portable medium such as a smart card)

(j) Two or more banks operability (the electronic money scheme can be used in common by a number of banks)

3. Typical Scheme

The electronic money schemes presented hitherto do not satisfy all the requirements described in Chapter 2. Because of the particular situation in which it is intended to be used, each electronic money scheme is uniquely designed giving different emphasis to the importance or priority of each requirement. Of course budget constraint is another important

factor which restricts the satisfaction of these requirements. In the course of future development toward more practical use, competition between these various electronic money schemes is expected to stimulate innovation. Many experts think that a number of schemes with different features will coexist.

BIS (1996) surveys existing electronic money products and highlights the main design features and functional aspects of these products and analyses the technical risks specific to individual types. It also presents some possible security measures that can be relied upon to prevent, detect and contain fraud. For more information, please refer to the report.

Okamoto and Ohta (1993) discussed the requirements for electronic money theoretically for the first time and showed that electronic money that satisfies them can be constructed using a note-based model. Fujisaki and Okamoto (1996) improved this scheme so that it could be implemented on a smart card basis. This system guarantees user's privacy by establishing a trusted third party (not involved in the electronic money transaction). It also adopts a standard digital signature to make the money transferable, reducing the volume of data processing as well as telecommunication traffic, which reduction made withdrawal and payment by a smart card possible. However, this scheme had the following problems:

(1) Since the post-transaction detection method was the main protection against overspending, prevention measures against such invalid use were not sufficient.
(2) Since each bank issued its own electronic money in this system, people having accounts at different banks could not use the same money scheme.
(3) Data of all spent electronic money had to be stored in the bank's database to detect overspending. Therefore, there was a problem of the database becoming extremely large as the amount of money issued grew.

4. Design principles

This chapter illustrates a design for a new electronic money scheme that satisfies all the requirements described in Chapter 2. Fujisaki and Okamoto (1996) already satisfies the following requirements: (b) identifying malicious users, (c) divisibility, (d) over-the-counter and over-a-network payment capability, (f) privacy protection, (g) off-line operability, (h) direct transferability between individuals, and (i) portability. By adding new ideas to this scheme and extending it, a new electronic money scheme satisfying all the requirements can be achieved.

The following are the basic principles we present in order to satisfy these requirements that Fujisaki and Okamoto (1996) did not.

(1) Security

As a technological means for preventing invalid use such as overspending, the physical integrity of the smart card during the payment procedure has been adopted in this scheme in addition to the post-transaction detection method (identifying a malicious user), which is based on cryptographic technology and presented in Fujisaki and Okamoto (1996), Eng and Okamoto (1995), and Okamoto and Ohta (1990). Previous electronic money payment schemes using the zero knowledge proof [Eng and Okamoto (1995), Okamoto and Ohta (1990)] did not allow smart card implementation because of excessive computation and data volume. By simplifying the procedure used to prevent overspending using an efficient signature scheme, payment can be realized quickly enough even with general-purpose smart cards.

However, there is a possibility that the tamper resistance of a smart card may be defeated if sufficient money and time are available. Invalid use such as “hit and run” is possible if only a post-transaction detection method is adopted for security. By combining the pre-transaction and the post-transaction measures, multiple protection against various types of overspending can be realized. For example, overspending is already very difficult for ordinary people just because of basic smart card device techniques, and even if a smart card is analyzed and forged at high cost, such forgery can be detected by the post-transaction detection method with cryptographic techniques. These security measures can be flexibly combined depending on the size of payments, budget constraints and other conditions.

(2) Privacy protection

In the process of a payment of electronic money, a certificate issued by the registration center is shown to the payee instead of the payer’s information (payer’s real name, etc.). Untraceability is achieved because only the registration center knows the real name of the holder of the certificate (payer).

If necessary, unlinkability is achieved by registering before every withdrawal of electronic money, obtaining different certificates each time even if the withdrawer is the same person.

(3) Common electronic money shared by a number of banks

For the convenience of customers, and the efficiency of the society as a whole in the administration of electronic money, a number of banks are allowed to share a common electronic money system. For this purpose, a new institution, which specializes in issuing

electronic money, is introduced. The settlement of common electronic money between banks can be done through this institution thereby allowing a number of banks to exchange common electronic money. Each individual holds an account at a bank and withdraws an amount from the account, in order to obtain electronic money. The issuing institution will send the electronic money to the individual at the bank's request following the withdrawal from the individual's account. Only the issuing institution has the database of outstanding electronic money and checks the validity of newly returned money from the banks.

(4) Efficient management of the electronic money system

The database size of the outstanding money at the issuing institution has been reduced, while at the same time the customers' privacy is preserved. In the earlier electronic money scheme of Fujisaki and Okamoto (1996), upon issuing electronic money, the issuing institution authenticates electronic money by using a cryptographic technique called "blind signature" in order to block pursuit of a user's purchase history. When electronic money is issued using blind signatures, the issuing institution cannot see the identification number given upon each issuance of electronic money, which is contained in the electronic money. Therefore the issuing institution cannot utilize the identification number for administrative purposes.

We have presented a new scheme to deal with this problem, in which only banks use blind signatures and the issuing institution uses general digital signatures. The procedure of acquiring electronic money by withdrawing it from one's bank account consists of two steps: (i) obtaining a ticket from the bank from which one is making a withdrawal, and (ii) obtaining electronic money from the issuing institution by submitting the ticket.

In order to prevent the bank from connecting user information, such as the user's real name and account number, obtained upon withdrawal from an account held there, to the electronic money information, "blind signature" is used when the ticket is issued. When a user accesses the issuing institution to obtain electronic money, the user needs to submit only the ticket, and other user information such as the user's real name need not be given. Hence, the issuing institution cannot connect the electronic money information to the user information, and the user's privacy can be protected by using not a blind but a general digital signature.

To check invalid use, such as an overspending of electronic money, previous systems had to store records of all issued money in the issuer's database. But in this new scheme, money is recorded in the database when issued and is deleted from the database when returned to the

issuing institution through the banks. The database holds only the data of currently outstanding money and if some money not included in the database returns, it can be considered as invalidly used. Hence, the size of the required database storage resources can be dramatically reduced compared to previous methods.

5. Protocol

This electronic money scheme is constructed based on the design principles described in the previous chapter. An outline of the new scheme is given below. Figure 1 provides an overview. The thick lines represent the flow of electronic money.

First, the function of each node is explained. The registration institution is the institution with which the user registers beforehand in order to use electronic money and this institution verifies that the user is the legal holder of the electronic money. The issuing institution issues electronic money, manages it, and detects invalid use of it. Banks manage the users' accounts and issue tickets to withdraw electronic money from the issuing institution at a user's requests. Users withdraw, pay, and deposit electronic money.

Next, the process of the scheme will be explained using Figure 1.

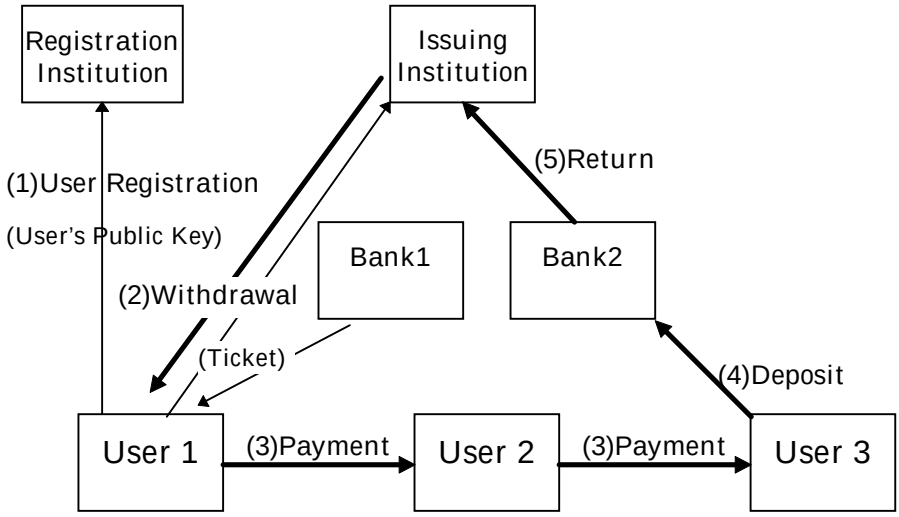

Figure 1. Overview of the new electronic money scheme

(1) Registration of users

The registration process is the phase in which certificates necessary for use of electronic money are generated. The protocol for this is shown in Figure 2. First, the user creates a secret key to be used in producing signatures, and then creates an associated public

key. The user sends the public key and his/her real name to the registration institution. The registration institution records the received public key and the user's real name in its database and then creates a digital signature of the public key and sends it back to the user (hereafter these digital signatures are called certificates). In the following payment protocols, the payer presents his/her public key and his/her certificate to the payee. The payee can verify that the payer is a genuine user who has registered with the registration institution by checking that the certificate is the digital signature of the registration institution for the payer's public key. On the other hand, the payer's privacy is protected since his/her real name is not disclosed.

In order to ensure the untraceability presented in Chapter 2, the registration process is required to take place only once, upon entering the system. If the unlinkability also presented in Chapter 2 is required, the user must register before every withdrawal process.

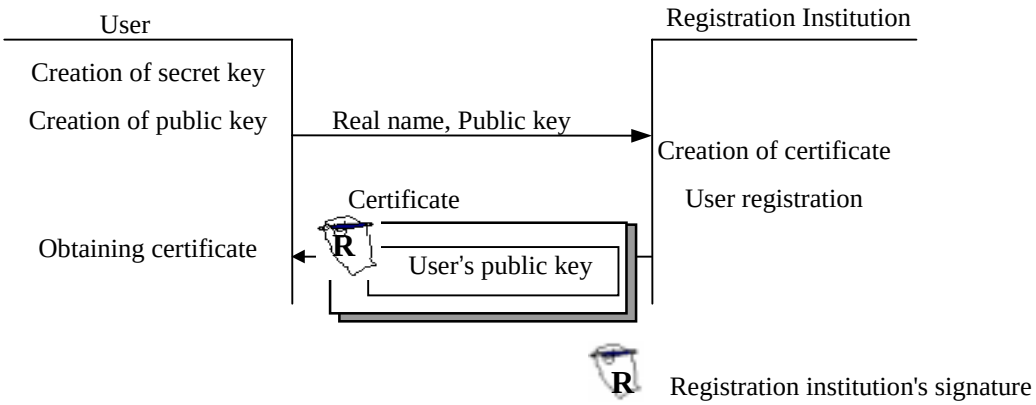

Figure 2. Protocol of registration processing

(2) Withdrawal of electronic money

In this phase the user accesses to the bank and the issuing institution to obtain electronic money. The protocol is shown in Figure 3. The procedure of withdrawing electronic money consists of two steps: (i) obtaining a request ticket from the user's bank, and (ii) obtaining electronic money from the issuing institution by submitting the request ticket (Figure 3).

(i) Obtaining a ticket from the bank where users hold their accounts

After the user and the bank are mutually certified, the user sends his/her account number and the amount of the withdrawal to the bank. The bank sends its public key corresponding to the amount of withdrawal to the user. Then the user blinds his/her public key using a blinding function and sends it to the bank. The bank deducts the amount of withdrawal from the user's account and produces a digital signature of the user's blinded public key and sends it to the user. The user unblinds the bank's digital signature and obtains the request ticket.

(ii) Obtaining electronic money from the issuing institution by submitting the ticket

The user approaches and certifies the issuing institution, and sends the request ticket, the certificate and the user's public key to the institution. The issuing institution checks the signatures received, and creates its digital signature on the administrative number of the electronic money, the amount issued, and the user's public key. The digital signature is in fact the electronic money and is sent to the user following storage in the issuing institution's database.

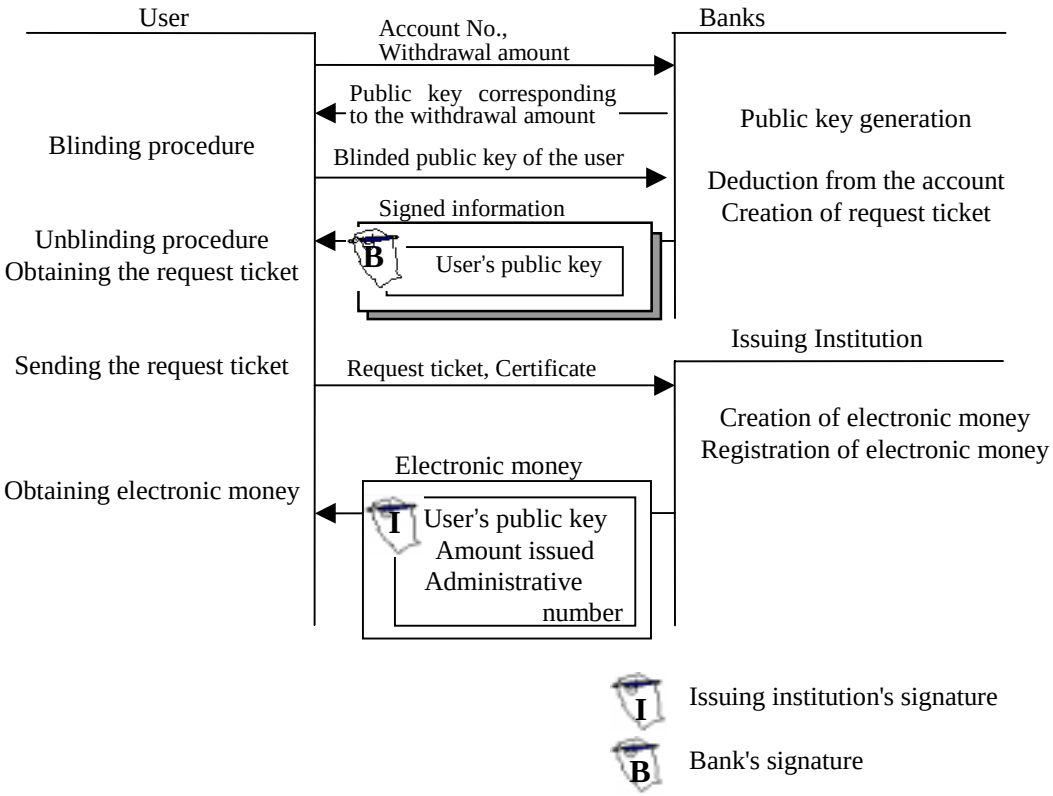

Figure 3. Protocol of withdrawal

(3)Payment (or transfer) of electronic money

In this phase payment is processed. The protocol is shown in figure 4. It should be noted that electronic money first consists only of the signed information obtained from the issuing institution, but as it is used, the transaction records are added and these records are added to the original information included in the electronic money. The payer presents the certificate, the payer's public key, and the electronic money information to the payee. The payee checks the certificate and makes sure that the payer's public key is identical to the one registered at the registration institution. He/She also checks that the electronic money information is formed properly, i.e. checks whether the money was issued to a genuine user

by the issuing institution, and checks if the transaction process was proper if it has transaction records.

Next, the payee sends information consisting of a random number and the payer's name and his/her public key specially modified, to the payer as a piece of information. The payer creates his/her digital signature on certain information including challenge information, and sends it to the payee.

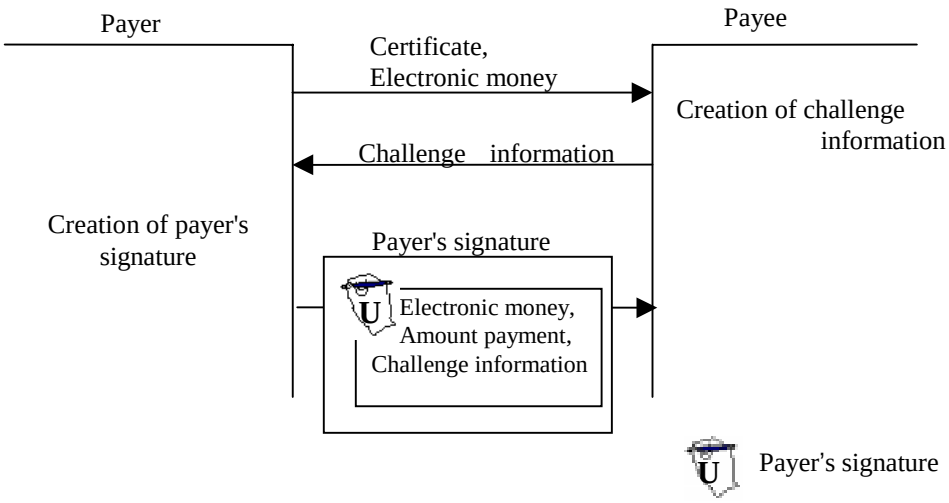

Figure 4. Protocol of payment

(4) Deposit of electronic money

The deposit process is accomplished by transferring all information obtained in (3) to the bank (Figure 5).

(5) Return of electronic money

The return process is achieved by transferring the information that the bank obtained in (4) to the issuing institution (Figure 6).

(6)Identification of a malicious user

All the transaction records will be returned to the issuing institution from the banks. The records will be managed by the administration numbers given upon each issuance of the electronic money. First the institution extracts the information of the amount spent. If the money has been divided and spent, the amounts of the payments are added up. The sum and the amount issued are compared and if they are the same, the records of the electronic money are deleted from the database and kept in the backup. If some money that was not recorded in the database returns, or the sum of the payments exceeds the amount issued, some invalid

use will be considered to have occurred. In this case, the public key of the suspect would be extracted, and this would be sent to the registration institution with corresponding signature information. The registration institution would identify the malicious user by finding the name of the user of the public key from its database.

6. Evaluation

This chapter shows in summary form that the requirements described in Chapter 2 are in fact satisfied in the proposed electronic money scheme.

Table 1. Evaluation of the Proposed Electronic Money Scheme

Requirements	Method of Treatment
Security	
Preventing invalid use	Prevent invalid use by employing the tamper resistance of smart cards
Identifying malicious users	Use cryptographic techniques such as digital signature to prevent forgery, or identify malicious users
Unique convenience	
Divisibility	Achieve breakdown into desired denominations by inputting the payment amount into the payer's signature
Over-the-counter and over-a-network payment capability	Because the value comprises only information and is stored in a smart card, payment not only over-the-counter but also over a network is possible
Efficiently managing the issuing of electronic money	Minimize the amount of data in the electronic money management database by employing a method that records the issued electronic money which has not yet been returned to the database and deletes it from the database upon return.
Inheritance of merits from cash	
Privacy	
Untraceability	Protect user privacy by establishing a registration institution and using blind signature
Unlinkability	Can be achieved by conducting registration processing before every withdrawal and using different certificates
Off-line capability	Perform electronic money transaction by transacting parties (payer, payee) verifying each other's signature information, etc, when payment is made
Direct transferability between individuals	A sequence of user's signatures added upon each transfer makes this feature possible.
Portability	Minimizing the amount of processing and data enables payment and receipt of electronic money through smart cards, etc.
Two or more banks operability	Separating the issuing institution and the banks enables electronic money to be shared in common by a number of banks

Reference

(in English)

Abe, M. and Fujisaki, E., "How to Date Blind Signatures," Advances in Cryptology-ASIACRYPT'96, LNCS 1163, Springer-Verlag, pp.244-251, 1996.

BIS, "Security of Electronic Money," Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the Central Banks of the Group of Ten Countries, Aug 1996.

Brands, S., "Untraceable Off-line Cash in Wallet with Observers," Advances in Cryptology-CRYPTO'91, LNCS 773, pp.302-318, Springer-Verlag, 1993.

Chaum, D., "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," Communications of the ACM, Vol.28 NO.10, pp.1030-1044, 1985.

----------, A.Fiat and M.Naor, "Untraceable Electronic Cash (Extended Abstract)," Advances in Cryptology-CRYPTO'88, LNCS, No.403, Springer-Verlag, pp.328-335, 1989.

Eng, T. and Okamoto, T., "Single-Term Divisible Electronic Coins," Proc. of EUROCRYPT '94, LNCS 950, pp. 306-319, Springer-Verlag, 1995.

Even, S., Goldreich, O., Yacobi, Y. "Electronic Wallet," Proc. of CRYPTO'83. A later version appeared in Proc. of 1984 International Zurich Seminar on Digital Communications, pp.199-201, IEEE cat No.84CH1998-4.

Matsumoto, T., "An Electronic Retail Payment System with Distributed Control - A Conceptual Design -," IEICE Trans. Fundamentals, Vol.E78-A, No.1, 1995.

Okamoto, T. and Ohta, K. "Divertible Zero-Knowledge Interactive Proofs and Commutative Random Self-Reducibility," Advances in Cryptology-EUROCRYPT'89, LNCS 434, pp.134-149, Springer-Verlag, 1989.

----------, and ----------, "Disposable Zero-Knowledge Authentications and Their Applications to Untraceable Electronic Cash," Proc. of CRYPTO '89, LNCS 435, pp.481-496, Springer-Verlag, 1990.

----------, and ----------, "Universal Electronic Cash," Advances in Cryptology-CRYPTO'91, LNCS 576, pp.324-337, Springer-Verlag, 1991.

(in Japanese)

Abe, M., and Camenisch, J., "Partially Blind Signature Schemes," 1997 Symposium on Cryptography and Information Security, SCIS97-33D, 1997.

Okamoto, T. and Ohta, K., "Risou Teki Denshi Genkin no Ichi Houhou," Trans. of IEICE, J76-D-I, No.6, pp.315-323, 1993.

Nakayama, Y., "Denshi Kessai ni Tsuite," International Telecommunication Union Journal, Vol26, No.7, pp.54-62, Sin Nippon ITU Kyokai, 1996.

Fujisaki,E., and Okamoto, T., "Escrow Electronic Cash," Trans. of IEICE, IT95-51, ISEC95-46, SST95-112, pp.7-12, 1996.

Moribatake,H.,Abe,M., Fujisaki, E., and Nakayama, Y., "Electronic Cash Scheme," 1997 Symposium on Cryptography and Information Security, SCIS97-3C, 1997.