Global Co-Operation in the New Millennium
The 9th European Conference on Information Systems
Bled, Slovenia, June 27-29, 2001

CURRENCY EXCHANGE SYSTEM FOR ELECTRONIC MONEYS

Yoshitaka Nakamura

NTT Information Sharing Platform Laboratories, 1-1 Hikari-no-oka, Yokosuka-shi, Kanagawa, 239-0847 Japan
Tel.: +81 468 59 2145, Fax: +81 468 59 8329
yoshitaka@isl.ntt.co.jp

Takeshi Nagayoshi

NTT Information Sharing Platform Laboratories, 1-1 Hikari-no-oka, Yokosuka-shi, Kanagawa, 239-0847 Japan
Tel.: +81 468 59 2120, Fax: +81 468 59 8329
nag@isl.ntt.co.jp

Takuo Nishihara

NTT Information Sharing Platform Laboratories,1-1 Hikari-no-oka, Yokosuka-shi, Kanagawa, 239-0847 Japan
Tel.: +81 468 59 2064, Fax: +81 468 59 2241
tac@isl.ntt.co.jp

ABSTRACT

A currency exchange system is introduced for a multi-currency electronic money trial, in which smartcard-based electronic moneys (two currencies) are circulated over the Internet. Considering the need to support our existing single currency electronic money protocol, the exchange method proposed herein offers fairness between untrusted parties based on the "optimistic approach". This paper describes the concepts and basic specifications of the currency exchange system as well as evaluation results of the trial held from October 1999 to March 2000.

1. INTRODUCTION

A number of electronic payment systems have been proposed for the Internet (Chaum et al. 1988, eCash, Mondex, MilliCent, SET). Each existing system has its own characteristics which are analyzed in (BIS 1996), such as card-based/software-based, "note-based"/"balance-based", personal transferability, offline/online, anonymity, and traceability.

As those payment technologies support business and personal activities over the Internet, a wide variety of commercial transaction services are emerging. Electronic money is being exchanged for not only physical goods but also digital values including multimedia contents, digital rights as tickets (Fujimura and Nakajima 1998), or digital coupons. Furthermore, if electronic money can be transferred from shops to customers, electronic money itself can be purchased through currency exchange services.

While most payment systems are designed to assure the integrity and authorization of the value of money, a number of studies have addressed "fairness" in the exchange of digital values (Asokan et al. 1997, Asokan et al. 1998, Asokan 1998, Ben-Or et al. 1990, Cox et al. 1995, Deng et al. 1996, Franklin and Reiter 1997, Zhou and Gollmann 1996). The definition of *weak fairness* is to guarantee that at the end of the exchange, either each party has received what it expects to receive or one party can prove to an arbiter by himself that the other party has received the expected value. *Weak fairness* can be achieved by assuring *non-repudiation of agreement* and *non-repudiation of receipt*.

In this paper, we describe the implementation of a currency exchange system that realizes fair electronic value exchange between untrusted entities over an open network. This implementation is being confirmed in a multi-currency trial, one part of a more comprehensive electronic money trial, Step2 trial (Toramatsu et al. 2000). The electronic money system in the trial is a note-based, card-based, offline, transferable, pseudonymous and traceable electronic money system based on NTT electronic money technology (Okamoto et al. 1998, Okamoto and Ohta 1990, Moribatake et al. 1998). The Step2 system was connected to the Japanese banking system and was in service in Japan from April 1999 to March 2000 after a successful half-year preliminary trial (Step1) from September 1998. A brief review of NTT electronic money and the trial system is given in section 2; please refer to (Toramatsu et al. 2000) for a detailed discussion.

The multi-currency trial including the currency exchange service was conducted from October 1999 to February 2000 as a part of the Step2 trial. Its aim was to confirm the applicability of our electronic money technology to international electronic commerce. The concept of the multi-currency trial and the currency exchange function are introduced in section 3.

In implementing the currency exchange system, we adopted the concept of "optimistic fair exchange" proposed in (Asokan et al. 1997, Asokan et al. 1998, Asokan 1998), and developed a method that supports the existing payment specification of the Step2 trial. The *Optimistic approach* does not require a third party to be involved in ordinary cases, but when exceptional cases occur, such as accidental breaks and intentional interruptions by dishonest participants. Basic specifications of the currency exchange system including the exchange method and an analysis of fairness are described in section 4. A brief evaluation of the trial results is given in section 5.

Throughout this paper, "public key" means the key for verifying digital signatures generated by the corresponding "secret key". In fact, public keys in our scheme should be published, however, not with a certificate that shows owner's private data such as real name, affiliation etc., instead a license that shows only the public key and its digital signature created by the licenser's secret key is used. Therefore, the release of one's public key or license does not mean the breakage of her/his privacy.

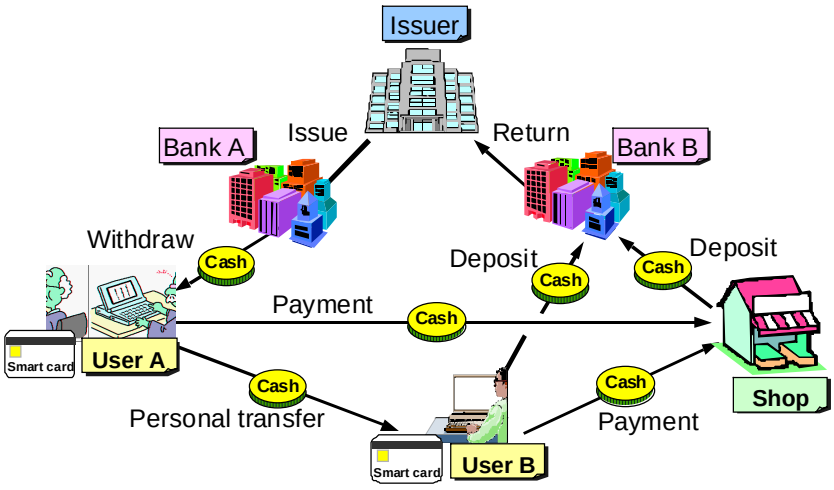

Figure 1: *Basic scheme of NTT electronic money*

2. BRIEF REVIEW OF THE TRIAL SYSTEM

The basic scheme of NTT electronic money is shown in Fig. 1. The issuer is an organization that issues electronic money and users' licenses, and it detects illegal use when electronic money is returned. It clears electronic moneys distributed by several banks. Each bank issues smartcards and manages its own users' accounts and deals with users' requests for deposits and withdrawals of electronic money. Each registered user has a smartcard and makes offline payments to shops or other users over the Internet. Most shops do not have their own smartcards but use "payment servers" which receive payments from users and deposit them in each shop's bank account. In our scheme, the issuer and the banks are considered to be service providers and so are trustworthy, but users and shops are considered to be service users and thus untrustworthy.

The main characteristics of the system are as follows.

A. Advanced Security

On the users' side, the integrity and confidentiality of core processes and secret keys are protected by the tamperproof property of the smartcards. Furthermore, a digital signature of the payer, "payment signature", which indicates that the payment is intended for the payee is attached to the original electronic money data in each payment. This chained signature scheme makes it possible to detect overspending and to identify the guilty party's public key when the electronic money data returns to the issuer. This means that NTT electronic money can be applied to offline payments. This traceability is designed to protect users' privacy up to the level of pseudonymity. In our scheme, in usual situations, users are identified only by their public keys which act as pseudonyms, information such as real name, address, bank account and so on remain hidden. Personal information of a user is known only by the bank, which does not know the linkage between users' public keys and their bank accounts. However, when illegal use is detected the issuer and the bank cooperate and identify the real name of the guilty party.

B. Personal Transfer

Users can conduct personal transfers by themselves; there is no need for a third party such as a bank server. Especially in this trial, users can send money via E-mail, which enables electronic money data to be transferred through firewalls and does not require synchronous connections between the payer and the payee.

C. Resumption and Refund Mechanism

As the communication quality of the network and the stability of PCs are still unreliable, we must take into account accidental interruptions of communication during money operations. It is impossible in our electronic money scheme to cancel a transaction after the creation of a payment signature by the payer's smartcard or the withdrawal request is accepted by the real banking system. A transaction resumption mechanism was developed which enables any interrupted transaction to be continued from the state just prior to the interruption; the smartcards are locked until the transaction is resumed and completed.

We also provided a refund operation for owners of revoked smartcards though this means restricting the open-loop nature of our original scheme. A detailed description of this operation is given in (Toramatsu et al. 2000).

3. CONCEPTS OF THE MULTI-CURRENCY TRIAL

The multi-currency trial was planned to confirm the applicability of our electronic money scheme to international trade and discover the technical and legal issues.

The technical requirements for the multi-currency trial system are as follows,

- to issue and circulate electronic money in US dollars (USD) along with existing electronic money in Japanese yen (JPY),
- to provide users with a function that exchanges USD for JPY and vice versa so that users do not need to have USD bank accounts, and
- to minimize the impact on the existing Step2 electronic money system.

3.1. Multi-Currency Support

Additional currencies can be supported simply by duplicating and extending the system originally developed for Japanese yen; only the currency unit needs to be changed. One or more banks must hold reserves of the new currency and to issue electronic money in that currency. Users are not required to have a bank account in the new currency because currencies can be converted through the currency exchange service as described below. However, an operational requirement requires multi-currency users to have one smartcard for each currency; it is technically possible to load multiple currencies into one smartcard.

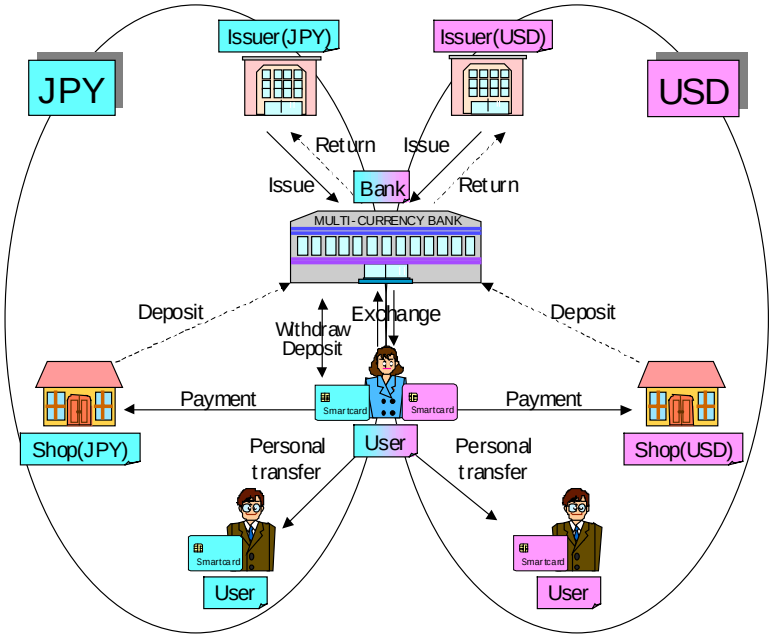

Figure 2-a:. *Exchange service provided by a bank*

3.2. Currency Exchange Service

The following two models are possible as a currency exchange system.

Exchange service provided by a bank

In this model, the bank system issues electronic money in USD to users in exchange for the users' deposit of electronic money in JPY and vice versa as shown in Fig. 2-a. This model has the following advantages:

- the exchange service provider is assumed to be trusted by users, so that fairness need not be addressed;

There are two disadvantages:

- existing bank servers used in Step2 service should be modified to handle currency exchanges;
- providers of the currency exchange service are restricted to the banks registered as distributors of electronic money in JPY;

Exchange service provided by an untrusted entity

It is possible for any two users to exchange their electronic moneys using the personal transfer mechanism of NTT electronic money. The second model is an enhancement of this concept. In this model, an exchange agent, who has shop functions as well as personal transfer functions, provides the currency exchange service. This model is shown in Fig. 2-b.

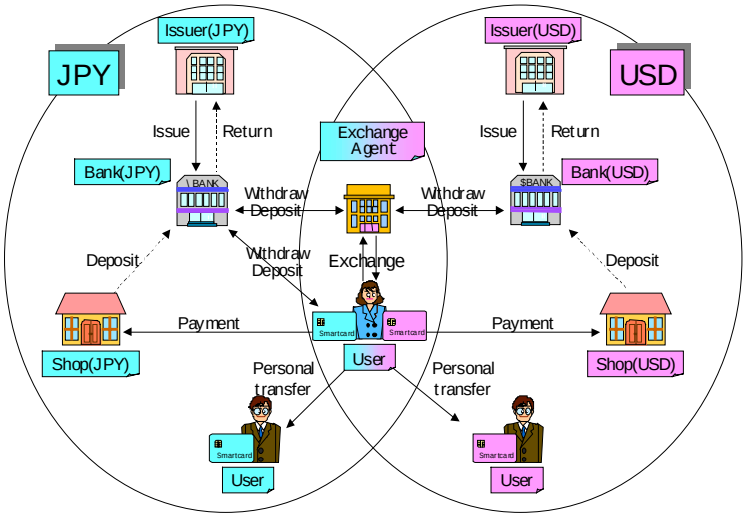

Figure 2-b: *Exchange service provided by an untrusted entity*

The exchange agent has a certain amount of electronic money stored in its smartcards in advance, and pays the equivalent amount of electronic money from them, using the personal transfer mechanism after the payment from the user is completed.

This model has the following advantages:

- it is enough for the bank server to handle just one currency, so that the existing Step2 bank system program need not be modified;
- as the functions for bank and exchange transaction are separated, this model has high flexibility because the exchange service could be provided by any entity, even banks.

This model has the following disadvantage;

- the service provider may be considered untrustworthy by some users.

We adopted the second model because its disadvantage can be overcome by technical advances while the disadvantages of the first model can not.

The selected model is possible by virtue of the personal transferability of NTT electronic money. Exchange transactions are processed totally offline from the issuers of both currencies, so this model supports the concept of NTT electronic money that payment need be monitored by the electronic money provider, the issuer or the banks.

Moreover, in the future, this model can be easily applied to extended exchange systems in which various kind of electronic values such as electronic moneys, electronic tickets, digital rights and so on are exchanged. We have a vision that rights-managed digital contents will also become items handled by extended exchange systems, and these systems will become an important infrastructure for the distribution of digital contents.

3.3. Optimistic Fair Exchange

In the selected model, a serious problem is how to guarantee fairness in transactions given that there is only a limited level of trust between users and the exchange agent. We should consider the risk of injustice such

that the debtor may escape after receiving values or repudiate the receipt of values, a malicious third party may intercept the values, and the creditor may demand double payment by spoofing an interception by a third party.

We adopted *the optimistic approach* in designing our fair exchange system. The optimistic approach is a concept to reduce the overhead of risk management, no TTP (trusted third party) is required except when transactions can not be well completed; this differs from the more strict approaches. However, the optimistic fair exchange protocols in (Asokan et al. 1997, Asokan et al. 1998, Asokan 1998) are not suitable for our intent because they were designed for exchanging restorable items when the exchange was aborted after issuing the commitment. In our case, the items being exchanged include signed data on a payment challenge as a commitment of payment, and the transaction cannot be aborted after making a payment signature for prevention of double spending. Therefore, we devised a method that suits our payment specification. Our policy is that fairness is achieved by setting evidence in the form of digital signatures step by step in the exchange transaction and thus one party can prove the illegal act of the other party by showing this evidence to a TTP such as the courts, if necessary. We did not actually implement the TTP system and instead replaced it with manual execution in this trial to lower the cost; this means that the timeliness required in (Asokan et al. 1997, Asokan et al. 1998, Asokan 1998) is not assured automatically.

4. BASIC SPECIFICATION OF THE CURRENCY EXCHANGE SYSTEM

As shown in Fig. 2-b, the issuers, banks, payment servers, and smartcards need to handle only one currency, JPY or USD. Additional modules to handle multiple currencies are the wallet software of the users' systems and the exchange server system.

The currency exchange transactions consist of three phases: *negotiation*, *the first payment*, and *the second payment*. Here the first and the second payment are the payment from the user to the exchange agent and the opposite, respectively. In the negotiation and the 2nd payment phase, users access the exchange server, and in the 1st payment phase, users access the existing payment server of the Step2 system, which is shared by several shops and the exchange agent. The 2nd payment is based on the personal transfer mechanism.

The structure of the currency exchange system is shown in Fig. 3. The user system, which handles two smartcards, the exchange server, and two payment servers communicate via the Internet. The exchange server controls and manages information such as the status of transaction and the payment history of the exchange agent's smartcards.

Apart from keys for electronic money payment, each smartcard and server has another key pair. These keys ensure the security of commercial transactions such as the fair exchange method as follows.

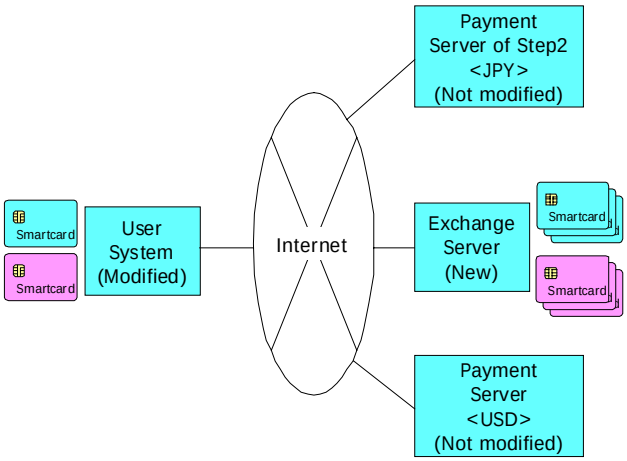

Figure 3: *Structure of the currency exchange system*

4.1. Protocol

The currency exchange protocol is shown in Fig. 4, which illustrates the example of changing JPY into USD.

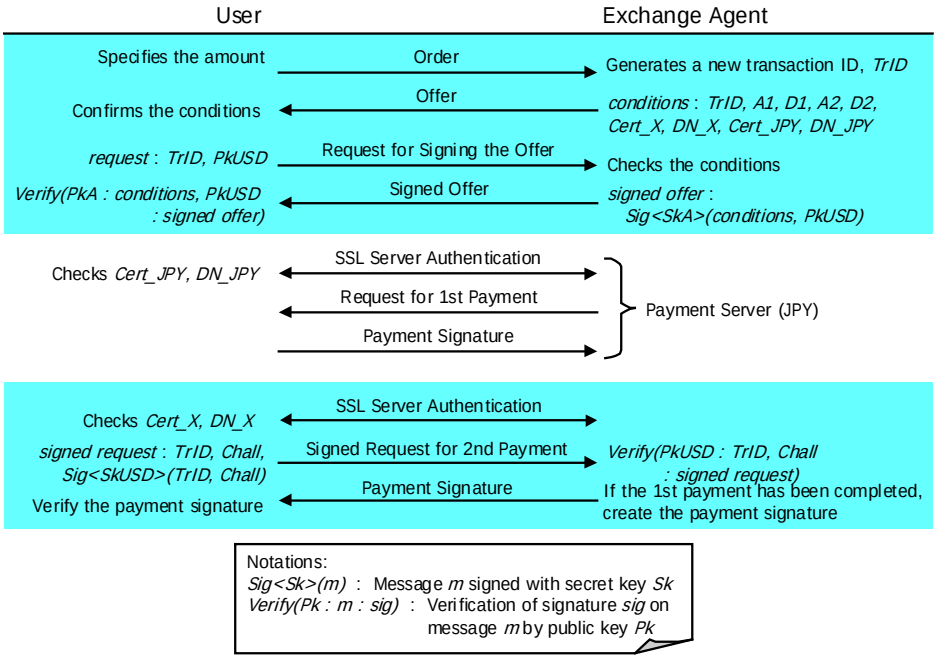

Figure 4: *Protocol of currency exchange*

Negotiation

First, the user accesses the web page of the exchange agent, refers the listed exchange rate expressed as payment amount in JPY for one USD, and specifies the amount to be exchanged. The exchange server then sends the conditions as an offer including;

- transaction ID, *TrID*,
- amount of 1st payment (amount of payment), *A1*,
- deadline of 1st payment, *D1*,
- amount of 2nd payment (amount of receipt), *A2*,
- deadline of request for 2nd payment, *D2*,
- certificates and distinguishing names of the exchange server and the JPY payment server, *Cert_X*, *DN_X*, *Cert_JPY*, *DN_JPY*.

If the user agrees to the offered conditions, she/he sends a request for signing the offer; the request includes the transaction ID, *TrID*, and the public key for authentication of the USD smartcard, *PkUSD*, as an identifier of the valid receiver's smartcard. The exchange server digitally signs the conditions and the receiver's public key as a signed offer and returns it to the user. The user's system automatically checks that the conditions have not been altered and verifies the signed offer and the certificate of the server. If they are all valid, the negotiation is concluded, otherwise the user's system aborts it.

1st payment

In this phase, the user makes the 1st payment in JPY. The user accesses the JPY payment server which is named in the signed offer and authenticates the server over an SSL connection. The user then pays electronic money in JPY from her/his JPY smartcard. We do not describe the payment protocol from the smartcard to the payment server in this paper. Please refer to (Toramatsu et al. 2000) for details.

2nd payment

In this phase, the user receives the 2nd payment in USD and stores it in her/his USD smartcard. The user accesses the exchange server and authenticates the server over an SSL connection and sends the server a request for payment including transaction ID, *TrID*, and payment challenge, *Chall*, digitally signed by the secret key for authentication of the USD smartcard, *SkUSD*. The server verifies the digital signature by the public key of the valid receiver, *PkUSD*, fixed in the signed offer and confirms with the JPY payment server whether the 1st payment of this transaction has already been completed or not. If the exchange server confirms the validity of the receiver smartcard and the completion of the 1st payment, it then orders its smartcard to generate payment signature of the exchanged amount in USD and sends it to the user. It is notable that this protocol is realized as a simple variation of the personal transfer mechanism. Details of the personal transfer protocol of NTT electronic money are shown in (Toramatsu et al. 2000).

4.2. Fairness of Currency Exchange

The fairness of our protocol is discussed below.

Non-repudiation of agreement

Making the debtor issue a signed offer prevents injustices in value exchange transactions via the Internet. The signed offer forms a part of the transaction history, and prevents the repudiation of the agreement by the debtor. The basic role of a signed offer is to guarantee that the specified return will be provided when the specified value is paid. Note that it is especially important to fix the agreed exchange rate in the signed offer for such transactions since exchange rates vary over time. In our case, the exchange rate is fixed using a pair of amounts, payment and receipt, in each currency.

Non-repudiation of receipt

The main risks are two injustices: interception of the receipt by a malicious third party, and a double demand by the recipient. To prevent these injustices, the user must send a digital signature when requesting the 2nd payment, which includes the transaction ID, *TrID*, and the payment challenge, *Chall*, and is signed by the secret key of the receiver's smartcard, *SkUSD*, in which the corresponding public key, *PkUSD*, is fixed in the signed offer in advance. According to this method, no one but the valid creditor can receive the exchanged electronic money. Moreover, double demands are easily detected if another request is sent after the first one has been already received, because no one can repudiate the receipt if the debtor gives the valid payment signature for the valid challenge fixed in the signed request. Naturally, injustices by the exchange agent can be prevented by the same method, but we did not implement the same countermeasure against the exchange agent's repudiation of receipt because, in this trial, the payment challenge generated by a payment server, which is trusted because it is managed by the money service provider, includes information that identifies the shop.

Thus our currency exchange method, which is designed to offer weak fairness, satisfies both types of non-repudiation. At the end of the exchange transaction, the user receives the valid amount of exchanged currency if all goes well. There are sufficient *non-repudiation tokens*, a signed offer, a signed request for 2nd payment and a payment signature for assigned challenge, to prove the other party's dishonesty if necessary. Only the timeliness formulated in (Asokan et al. 1997, Asokan et al. 1998, Asokan 1998) is not satisfied because we did not implement an arbiter's system. In addition, our protocol also achieves pseudonymity because users are identified only by their public keys with no additional personal information.

4.3. Resumption Mechanism of Currency Exchange System

In this subsection, we describe the resumption mechanism for currency exchange transactions. In the case of single currency transactions, users' status information needed to resume interrupted transactions in roll forward status is stored on their smartcards, which are locked when an interruption occurs. However in this

multi-currency trial, users have two smartcards, JPY and USD, so the resumption mechanism for single currency transaction fails to cover currency exchange transactions.

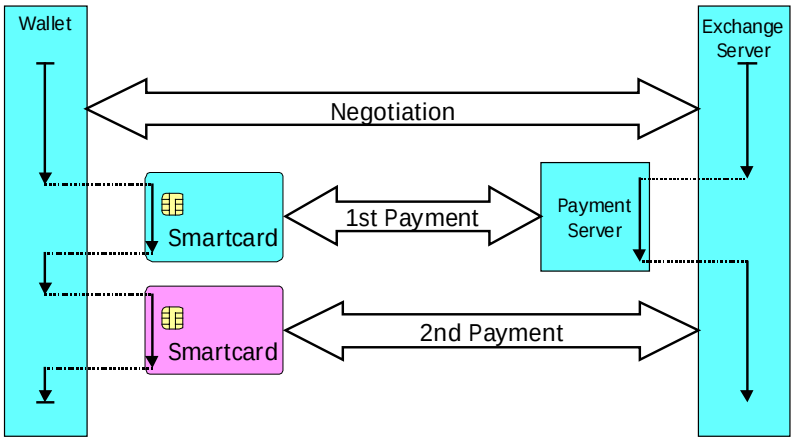

Figure 5: *Illustration of transaction management, solid arrows express the transition of the control.*

Users' systems (Wallet software)

The currency exchange transactions utilize the single currency smartcard functions for the 1st and 2nd payments. Therefore, the status information of each payment is stored on each smartcard and the rest should be stored on the users' PCs, such as the linkage between the two payments and the status information of the whole exchange transaction. The wallet software has a function to manage each exchange transaction as a whole by combining the two payment phases. Fig. 5 illustrates transitions in status information storage along the currency exchange sequence. According to this method, the smartcard used in the first payment does not need be locked as long as its own payment has been finished, and thus it can be used for other transactions.

Exchange server

In the negotiation phase, the server will not resume any interrupted transactions because no value is transferred at this point. An order is always treated as a new one and the exchange agent's server generates a new transaction ID for it.

In the 2nd payment phase, the critical point is the commitment of the request from the user. Once the server receives a valid signed request for 2nd payment, the payment signature will certainly be generated by using the payment challenge fixed in the request and will be stored in a database, and the exchange server will return the stored payment signature when the user resumes the transaction.

5. EVALUATION OF THE TRIAL

This multi-currency trial covered over three hundred registered users; one Japanese shop, two American shops and one Japanese bank handled USD. From the viewpoint of users' behavior, the cash-like usage of the electronic money was observed: users were apt to store their USD change in smartcards so as to use it at the next occasion; this minimizes the potential loss through re-exchanging into JPY.

There were no system troubles or injustices in the exchange transactions, and this result supports the practicability of optimistic fair exchange. Although the transaction management method adopted here has some risks in that a transaction may become unresumable if the users' hard disks crash at a critical point, those events did not occur during the trial. We prepared a refund operation for certificated owners of the receiver's public keys as a corrective measure in this trial, but of course it is desirable for all information needed for resumption to be stored on the smartcard when smartcards become to be able to load and manage multi-applications.

Some backstage operations of the exchange server, e.g. rate setting, were manually executed in this trial. Smartcard recharging is another such operation. The selected model of currency exchange service does not

prevent the *out of stock* problem because the exchange agent is just a retailer of electronic moneys and cannot carry an infinite amount of moneys, unlike banks. In actual operation, when out of stock occurs, the system warns the users and recharging is performed manually. Automatic recharging would eliminate this concern.

6. CONCLUSION

A currency exchange system was developed for a smartcard-based multi-currency electronic money trial on the Internet. Taking advantage of the personal transferability of NTT electronic money, we selected a system model that allows any entity to operate a currency exchange service. Using the concept of optimistic fair exchange, which enables exchange between untrusted parties, an exchange protocol was designed that supports the existing payment specification. The trial was successfully concluded and showed that the system achieves sufficient fairness for the exchange of electronic values over open networks.

REFERENCES

Asokan, N., M. Schunter and M. Waidner (1997). Optimistic Protocols for Fair Exchange. In Proceedings of the 4th ACM Conference on Computer and Communications Security, p. 7-17, ACM Press, Zurich.

Asokan, N., V. Shoup and M. Waidner (1998). Asynchronous Protocols for Optimistic Fair Exchange. In Proceedings of the 1998 IEEE Symposium on Research in Security and Privacy, p. 86-99, IEEE Computer Society Press, Los Alamitos.

Asokan, N. (1998). Fairness in Electronic Commerce. In his doctor thesis presented to University of Waterloo, Ontario, Canada.

Ben-Or, M., O. Goldreich, S. Micali and R. L. Rivest (1990). A fair protocol for signing contracts. IEEE Transactions in Information Theory, 36 (1), 40-46.

BIS, Task Force on the Security of Money, Committee on Payment and Settlement Systems, Group of Ten central banks, Bank for International Settlements (1996). Security of Electronic Money. Basle, Switzerland.

Chaum, D., A. Fiat and M. Naor (1988). Untraceable electronic cash. In Proceedings of the conference on Advances in Cryptology - CRYPTO'88, Lecture notes in Computer Science 403, p. 319-327, Springer-Verlag, Berlin.

Cox, B., J. D. Tygar and M. Sirbu (1995). NetBill security and transaction protocol. In Proceedings of the First USENIX Workshop on Electronic Commerce, USENIX, New York.

Deng, R. H., L. Gong, A. A. Lazar and W. Wang (1996). Practical protocols for certified electronic mail. Journal of Network and System Management, 4 (3).

eCash Technologies, Inc., eCash home, http://www.ecashtechnologies.com/

Fujimura, K. and Y. Nakajima (1998). General-purpose Digital Ticket Framework. In Proceedings of the 3rd USENIX Workshop on Electronic Commerce, p. 117-186.

Franklin, M. K. and M. K. Reiter (1997). Fair exchange with a semi-trusted third party. In Proceedings of the 4th ACM Conference on Computer and Communications Security, p. 1-5, ACM Press, Zurich.

Digital Equipment Corp., MilliCent White Papers, http://www.millicent.digital.com:8888/sell/white_papers/

MONDEX International Ltd., http://www.mondex.com/

Moribatake, H., H. Akashika, T. Suganuma and Y. Takahashi (1998). Hierarchical electronic cash scheme. In Proceedings of the 1998 Symposium on Cryptography and Information Security, SCIS '98-3. 1D.

Okamoto, T., H. Kawahara and K. Koyama (1998). NTT's public key cryptosystem and electronic money system. In Proceedings of Certicom Public Key Solutions'98.

Okamoto, T. and K. Ohata (1990). Disposable zero-knowledge authentication and their applications to untraceable electronic cash. In Proceedings of the 7th conference on Theory and Application of Cryptographic Techniques, Lecture notes on Computer Science, No. 435, p. 481-496, Springer-Verlag.

SET Secure Electronic Transaction, http://www.setco.org/

Toramatsu, K., T. Nagayoshi and Jy (2000). InternetCash System based on NTT Electronic Money. In Proceedings of the 8th European Conference on Information Systems, ECIS 2000, Vol. 2, p. 897-900.

Zhou, J. and D. Gollmann (1996). A fair non-repudiation protocol. In Proceedings of the IEEE Symposium on Research in Security and Privacy, p. 55-61, Oakland.