The endorsable electronic bank note —A currency on the Internet—

Shinsuke Miwa

School of Information Science,
Japan Advanced Institute of Science and Technology

February 14, 1997

Keywords: Electronic currency, Internet, Electronic signature, Encryption, Finalization.

There has been a significant growth in popularity of the Internet in last 3 years, and opportunities for various dealings to take place on the Internet has also grown significantly at the same time. On the Internet, these dealings are taking place internationally and on round the clock basis. Therefore, a settlement system that it is possible to make a 24-hour and international settlement is required.

Various systems are proposed and implemented. However, existing settlement systems on the Internet has three major drawbacks. First, some kind of server intervention on all settlements are required. Second, because the system is not capable of finalizing, requirements of the 24-hour settlement and the international settlement can not always be satisfied. Third, because the system is not capable of finalizing, there are additional financial overhead of finalization for users and settlement organization.

To conquer these drawbacks, in this paper, I proposed "the endorsable bank note (EBN)" method as an electronic currency system on the Internet. In this method, the EBN can be transferred in the rolling without server's intervention. The user settles by EBN transfer. In this scheme, the server only intervene in "Issue", "Verification" and "Exchange" of the EBN: server's intervention is not required in settlement between users. With this scheme, the concentration of the communication and processing load to the server can be solved.

Also, the bank note of this method has the possibility to become a currency on the Internet which can be finalized. The reason is as follows. Because a settlement is made by transferring, if the social trust in the whole system improves, the EBN can circulate only with the "Verification", without the "Exchange".

In the proposed method, the injustice can be detected, because the chain of the electronic signature of the user to be recorded into the body of the EBN. The chain of the electronic signature is encrypted so that users except for the verifying issuer are not capable of decoding the chain. Because of encryption, users can not obtain information of previous users of an EBN or alter an existing EBN. Also, the proposed method can restrain user of EBN from crimes and money laundering, because it is capable of detects injustices. If any injustice was to take place, the chain can be presented as an evidence.

Transactions in the proposed method are "Issue", "Endorsement", "Verification", "Exchange". The "Issue" is the issue of the EBN to a user by an issuer according to the request of the user. The "Endorsement" is to transfer an EBN from a user to another user. The "Verification" is the verification for the correctness of an EBN by an issuer requested by a user. The "Exchange" is the exchange of EBN for cash by an issuer requested by a user.

In the transaction of "Issue" and "Endorsement", an electronic signature is recorded in the EBN by the user. This is called "the endorsement information". The endorsement information is encrypted with the public-key of the issuer of the EBN. The user makes this encryption.

Because the user encrypts and records the endorsement information, the user may choose not to sign correctly or not to sign at all. To prevent this, the endorsement information is made by the cooperation of the payer and the payee. In other words, the endorsement information can not be made with either one. This is done by the payer and the payee mutually signing a common session ID and exchanging them. The payer signs, encrypts and records the session ID which the payee signed. Similarly, the payee signs and records the session ID which the payer signed, encrypted and record. With this scheme, when either does an injustice, it can be detected in the "Verification", because the correct information is found in another record. This is the mechanism for the proposed method to detect injustices.

The proposed method was made into set of protocols and was implemented as a prototype system and its operation was verified.

The proposed method was compared with the other settlement methods. Comparison was made in the following viewpoints: (a) existence of implementation, (b) provision for anonymity, (c) provision for encryption, (d) needs for dedicated hardware, or (e) software, (f) requirement for server intervention.

The proposed method was compared against instances of "secure credit card transaction", "electronic currency" and "electronic check" method. the *FIRST VIRTUAL* and the *CyberCash* was taken for "secure credit card transaction", the *ecash* was taken for "electronic currency", the *NetCheque* was taken for "electronic check". The comparison also included the *MONDEX* system and the *Escrow Cash* method. The *MONDEX* system is not using the Internet, but included as an example of system that is in large scale experiment in the real world. The *Escrow Cash* is included as it is widely believed as one of the future mainstream method.

Some problems are pointed out on the proposed method: (a) it is impossible to provide anonymity to the issuer. (b) it is difficult to sustain social trust in the bank note because the injustice can be detected only after it is carried out. This paper proposes skeletons of solutions for these problems.

In addition, there are problems called "the confirmation of the reaching" and "the possibility of the finalizing", which are inherent to currency systems on the Internet, are addressed with partial solutions.

The Internet could be thought as an independent community. If it was to be equipped with a currency system with enclosed finalization capability, the Internet could then be an independent economy unit with characteristics of the original Internet that extends beyond physical frameworks of the real world. As real world economy and frameworks of states continue struggle to find their way toward the 21st Century, the new Internet that is an independent community and an independent economy unit may present a way for the future.