HOW TO REALLY CIRCULATE ELECTRONIC CASH ON THE INTERNET

by
Katsuhito Iwai

Professor of Economics, The University of Tokyo
7-3-1 Hongo, Bunkyo-ku, Tokyo, Japan 113
iwai@e.u-tokyo.ac.jp or iwai@ibm.net
August 28, 1995 (Japanese version: March 30, 1995)

1. An introductory remark

The recent world-wide explosion of the Internet community has encouraged many individuals and groups to propose a variety of electronic payment systems that can be used safely and efficiently for the economic transactions on computer networks. Some proposals are mere variations on the traditional credit card system. But the more ambitious ones are aiming at an electronic cash system which turns an electronic stream of numbers, the only "thing" moving on lines, into 'electronic cash', or 'e-cash', that can be spent directly on on-line commercial wares. One such attempt is the DigiCash system of David Chaum.[1] Since any message transmitted through the Internet is accessible to anyone who cares to look, and since any copied number is as good a number as the original one, the basic problem is to devise a copy-proof and cheat-proof transmission procedure among computer users. The DigiCash system has solved this by adopting the public-key cryptography for digital signatures that can secure the privacy of communicated messages as well as the authenticity of their communicators. It has also incorporated a device of blind signatures which assures the complete anonymity of its users.

The DigiCash system (and other schemes based on similar principles) perhaps comes closest to the ideal of e-cash. Yet it still falls short of attaining that. It is because its "digicash" is issued only in exchange for a real money deposited in the payer's bank account

---

[1] See, for instance, DigiCash bv., "DigiCash - Numbers That are Money: The ultimate electronic payment system for any application," 1994, info@digicash.nl; David Chaum, "Achieving Electronic Privacy," *Scientific American*, August 1992; David Chaum, "Security without Identification: Transaction Systems to make Big Brother Obsolete," *Communications of the ACM*, 28/10 (1985).

(or otherwise supplied), and once used for payment it is redeposited into the payee's bank account (or cashed into a real money by the payer's bank). In spite of its name the "digicash" does not circulate in the electronic world as dollar notes and hundred yen coins do in the real world. It is in fact more like a traveler's check or a prepaid card.

The purpose of this note is to suggest a way to turn the "digicash" into a real 'e-cash' which circulates forever among Internet users. Technically, it is a simple, indeed a trivial, extension of the basic ideas of the DigiCash system. Conceptually, however, it has some interesting implications for the metaphysics on money.

2. Orwellian e-cash system

If we look at a dollar note or a hundred yen coin, we can see immediately that it consists of three basic elements: a piece of paper or metal, an inscription that it is worth a dollar or hundred yens, and fine printings or elaborate engravings that make it hard to copy, namely, a material, a denomination, and cryptic marks. Our e-cash also consists of these three elements, but all in the form of numbers. The denomination is already a number. But to make a material out of a number and to make a number hard to copy both require the technique of the digital signatures in the public-key cryptography.

The public-key cryptography endows each network user with a pair of digital "keys" that work like the inverse to each other: messages encoded with one key can be decoded only with the other key. It is also known that to detect one key from the other is practically impossible. So, one of the keys can be made public, as long as the other is kept private. Then, to encode a message with my private key is tantamount to signing it digitally. It can only be decoded with my public key, thereby assuring my authorship. And to encode a message with your public key is tantamount to addressing it especially to you. It can only be decoded with your private key, thereby assuring its confidentiality.[2]

---

[2] In this footnote, I make the above explanation slightly more formal. Suppose that a pair of transformations, $D(N)$ and $E(N)$, satisfy the following three conditions: (1) $E(D(N)) = N$ and $D(E(N)) = N$ for any message N, (2) it is practically impossible to construct one from the other, and (3) it is easy to parametrize, then one of them, $D(N)$, serves as the encoding/decoding transformation with the private key and the other, $E(N)$, as the encoding/decoding transformation with the public key. Indeed, the first equation in the condition (1) says that a message encoded with a

Consider a bank that has decided to issue an e-cash of a certain denomination to one of the network users. This e-cash may be drawn from his deposit, if he has an account with the bank. But, even if he has no account, the bank can issue it as a price for its purchase or as an advance for credit or simply as a gift. In the first version of our system, it is the bank that takes an initiative of e-cash creation by generating a long random number first. This random number will serve as a "material" for the e-cash. We assume that before the whole process begins the bank has already stored in its computer as many pairs of digital keys as the number of possible denominations. The halves of the pairs are kept private, but the other halves have been distributed to all potential users as public keys with an instruction which key corresponds to which denomination. The bank then retrieves one of the private keys that corresponds to a given denomination, encodes the chosen random number with it, and sends the resulting cryptographic number to the network user. We thus have three basic elements -- a material, a denomination, and cryptic marks -- all incorporated into a single crptographic number, and it is this number that will function as an e-cash for the network user.[3] He of course has to check its authenticity by decoding it with the bank's public key that corresponds to the designated denomination. If a meaningful message is generated, he is sure that the number is what he wants and stores it in his computer.

Later our network user sends this e-cash to another network user as a payment for his on-line purchase. The second user checks its authenticity, just as the first user did, by de-

---

private key can only be decoded with the paired public key; and the second equation in (1) says that a message encoded with a public key can only be decoded with the paired private key. Furthermore, from the above two equations, we can trivially deduce the copy-proof, cheat-proof transmission procedure between two network users, *i* and *j*. It is based upon the following pair of equations: $C = E_j(D_i(N))$ and $E_i(D_j(C)) = N$, for any N. In these equations C is a crypto message transmitted through networks. Only user *i* can generate it by encoding N first with his own private key and second with *j*'s public key, and only user *j* can recover N from it by decoding it first with her own private key and second with *i*'s public key. (All the communications between network users in our e-cash system are assumed to follow this procedure.) According to the RSA cryptographic system, a pair of transformations, $N^d \pmod{pq}$ and $N^e \pmod{pq}$, where *p* and *q* being large prime numbers and *d* and *e* satisfying $de = 1 \pmod{(p-1)(q-1)}$, precisely satisfy the above three conditions. Then, *d* and *pq* will be used as a private key and *e* and *pq* will be used as a public key. Of course, *p* and *q* must never be made public. See R. L. Rivest, A. Shamir, L. Adleman, "Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* , 21/2 (1978).

[3] Formally, an e-cash can be expressed as $N^d \pmod{pq}$, where N is a random number serving its material and *d* and *pq* constitute a denomination-specific private key of its issuing bank.

coding it with the bank's denomination-specific public key. Here emerges, however, a fundamental problem associated with the making of a material out of a number. An e-cash is a number through and through, including its "material", and a copied number is as good a number as the original one. Even if the second user has received an authentic e-cash from the first, an identical e-cash in some sense still remains in the memory of the latter's computer, and there is no guarantee that he won't spend it again before she will. In order to prevent his double spending, the e-cash number in his computer, not all but the random number part that served as the "material", has to be buried dead. The simplest way to do so is to throw it into the open list of dead random numbers that will be forbidden for the future e-cash use. Of course, the buried random number has to be replaced by a fresh random number as a new "material" in order for the e-cash to continue its life. It is therefore necessary for our second network user send the e-cash just received to the bank for "renovation". The bank decodes it by its own denomination-specific public key, checks the recovered random number with the list of dead numbers, throws it into the list if it was not in the list already or otherwise warns the user of the duplicity, replaces it with a newly generated random number, encodes it again with the private key that corresponds to the same denomination as before, and sends back a new cryptographic number to the second network user. It is now her turn to spend this renovated e-cash for her payment with the third network user. And the process can continue indefinitely.

One may perhaps wonder at this point whether the above e-cash system has indeed delivered what it has promised. Since its e-cash returns to the issuing bank for renovation every time it changes its owner, can we really say that our e-cash is "circulating" among network users? The answer to this question, however, is affirmative. It is true that the "material" of the e-cash is forever renewed by declaring the spent one as dead and replacing it with a new one. Indeed, it can't be otherwise. For only in this way can we secure a property right over a number, which is after all a public good which can be shared by everybody. (This is like giving a patent to the use of a particular number. When the patent period expires, that number is made public and loses all its economic value.) But the important point is that

the "denomination" of the e-cash is carried alive from one network user to another. We all know that all that matters for a cash to be used as a cash is how much it is worth and not what it is made of. Indeed, our e-cash is nothing but an electronic carrier of the value, and it is the "value" that is actually circulating among network users. Our e-cash has thus achieved the purest form of cash, or the purest form of "money".[4]

3. Anti-Orwellian e-cash system

The e-cash system described in the preceding section should be an Orwellian nightmare to any individualist. The bank knows everything. It can trace who paid which e-cash to whom at what time simply by looking at the past communication records. The bank can at any time impinge on the individual privacy. Worse, since it shares the knowledge of the current e-cash number with its holder, the bank may at any time be tempted to abuse it. The second version of our e-cash system eliminates these possibilities by incorporating the idea of blind signatures.

Suppose again that a bank has decided to issue an e-cash to a network user. In this new version, however, it is not the bank but the network user that takes the initiative. He first generates not one but two random numbers. The first random number serves, as before, as the "material" for the e-cash, but the second random number now serves as its "blinding" factor. Both numbers are kept private. The user then "blinds" the former by the latter and sends the "blinded" random number to the bank.[5] The bank in its turn encodes the "blinded" random

---

[4] See Katsuhito Iwai, *Kahei-Ron (On Money)*, Chikuma-shobo, Tokyo, 1993, (in Japanese) for the general philosophical discussion, and Katsuhito Iwai, "The evolution of money: a search-theoretic foundation of monetary economics," *CARESS Working Paper* #88-03, University of Pennsylvania (Februrary 1988), for the detailed mathematical analysis of the "essence" of money and monetary economy. [Note: the latter paper is now published as "The bootstrap theory of money: a search-theoretic foundation of monetary economics," *Structural Change and Economic Dynamics*, vol. 7. No.4 (December 1996).]

[5] The above description of the blind signature protocol can be made more specific as follows. (See the references given in footnote 1 for detail.) Let N and R be two random numbers. To "blind" the former by the latter is simply to compute $NR^e \pmod{pq}$, where e and pq are a denomination-specific public key of the bank. If this number is encoded by the bank with the paired private key, d and pq, we have $(NR^e)^d = RN^d \pmod{pq}$; and if this second number is

number with the private key that corresponds to a given denomination, and sends back the resulting "blinded" number to him. If the network user divides it by the blinding factor, there emerges an e-cash of a given denomination he is able to spend. Note here that in this new version the introduction of the blinding factor prevents the bank from knowing the true e-cash number, thereby protecting it from any temptation to defraud the current e-cash holder.

When the second network user receives the e-cash from the first user as a payment, she has to send it to the bank for "renovation". But in this new version, she also has to generate two random numbers by herself and send the blinded random number simultaneously. The bank then decodes the received e-cash with its own denomination-specific public key, throws its random number into the list of dead numbers, replaces it this time with a new blinded number supplied by the user, encodes this blinded number with the private key of the same denomination as before, and sends back the resulting cryptographic number without knowing its real content. If the second network user divides it by her blinding factor, she is able to get hold of the renovated e-cash ready for spending. And the process continues indefinitely. Throughout the whole process, the bank has no way to connect the list of the dead random numbers already used as e-cash materials with the list of the blinded random numbers it has authorized as new e-cash materials. Hence, the privacy of the e-cash users is completely shielded from its inquisitive eyes.

It should now be noted that, once our e-cash is created, the only role the bank will play is that of a caretaker. An e-cash keeps circulating among network users and may never return to the account of the issuing bank. This is indeed the very reason why our e-cash has become a true e-cash, and not an electronic version of bank-certified note like the original DigiCash system. And even if the bank were asked by some user to convert it into an outside money, it has no obligation to comply that demand, unless it so promised at the inception. Our e-cash can be made an absolutely inconvertible currency. Why then is it able to circulate among network users? It is simply because it is accepted as an e-cash by every network user simply

---

divided by R, we obtain $N^d \pmod{pq}$. This is of course an e-cash of a denomination that corresponds to a given public key, e and pq.

because it is accepted as an e-cash by every other network user! (This bootstrap mechanism is the "essence" of money.[6]) In any case, all that is left for our bank to do once an e-cash is created is to monitor the list of dead "materials" and authorize a new "material" by signing it (literally) "blindly". Of course, this is the job that can be delegated to any specialized agency. Moreover, even the creation of e-cash is not an God-given privilege of the bank. It is in fact not hard to see that any institutions with Internet-wide reputation are in principle capable of creating e-cash. Hence, our e-cash system can be completely divorced from the banking business. And whether we like it or not, we now have a distinct possibility for the emergence of the government-managed inconvertible e-cash systems that supplement the traditional government-managed inconvertible currency systems in the real world.

Some additional remarks are in order. First, the e-cash system we have described above is only an on-line payment type. However, its extension to an off-line type along the line suggested by Chaum, Fiat and Naor seems rather straightforward.[7] Second, it is theoretically possible (but practically very cumbersome) to allow each e-cash user to divide an e-cash into small denominations or add many e-cashes into one or do some combination of these operations, as long as the values are adding up. We now know that what is actually circulating is the value itself.

4. A concluding remark

This note was originally written as a protest to a friend who dismissed the electronic cash system as no more than an electronically sophisticated prepaid card. Technically, there is nothing new in this note. Conceptually, I hope there is. In any case, I have already managed to change the mind of my friend.

---

[6] See the reference given in footnote 4.

[7] See David Chaum, Amos Fiat, Moni Naor, "Untraceable Electronic Cash," *Crypto '92*, LNCS 403, Springer-Verlag, Berlin, 1990.