Electronic Commerce

5. Cash Transactions

V Rajaraman

V Rajaraman is with the Jawaharlal Nehru Centre for Advanced Scientific Research and the Indian Institute of Science, Bangalore. Several generations of scientists and engineers in India have learnt computer science using his lucidly written textbooks on programming and computer fundamentals.

Part 1. What is E-Commerce?, *Resonance*, Vol.5, No.10, 13-23, 2000.
Part 2. E-Commerce System Architecture, *Resonance*, Vol.5, No.11, 26-36, 2000.
Part 3. Secure Messaging, *Resonance*, Vol.6, No.1, 8-17, 2001.
Part 4. Payment Schemes, *Resonance*, Vol.6, No.2, 6-13, 2001.

In this article we will discuss payment by cash for e-commerce transactions and micro payments for services received via the internet.

Introduction

In the previous part, we discussed payment by credit cards and cheques in e-commerce. The cost of each transaction using credit cards/cheques is quite large and it is thus not appropriate for low value transactions. We normally use cash for many transactions, particularly, low-value transactions. The currency system as we know it today evolved over centuries and is time-tested (see *Box* 1). The major advantages of cash are:

- It is guaranteed by the government and does not normally lose its value in the short range (except when there is hyper-inflation!).
- It is universally recognised as having value and accepted as legal tender.
- It can be carried around.
- Any person having cash can exchange it for goods or services without the help of a third party such as a bank.
- It is anonymous. Traders cannot normally say who gave a particular currency note.
- Privacy of transactions is ensured because of anonymity.

The major disadvantages of cash are:

- It is not safe. If you lose your purse you will be lucky to get your cash back.
- It is bulky. Governments do not normally print large denomination currency notes to prevent criminals from stealth-

Box 1: Evolution of Money

Trading at the dawn of civilization was by barter. One exchanged a measure of rice, for example, for a cubit of cloth. The obvious limitation of this led to the use of proxies for value. Various proxies such as leather seals, sea shells, and later gold or silver coins became instruments of trade. The development of printing resulted in printed currency notes. As paper notes have no intrinsic value, in early days governments had to have in their vaults gold equivalent to the amount of currency notes printed. This is no more necessary. Governments, however, control the value of money by monetary policies such as interest rate adjustment, issue of government bonds, devaluation, etc.

ily transporting large amounts of cash. Government of India only recently started printing Rs.1000/- currency notes. Ten years ago the largest denomination was only Rs.100/- to reduce black money transactions.

The purpose of electronic cash (abbreviated e-cash) is to mimic cash transactions with all its advantages without its disadvantages. The major problems, however, are:

- Who will issue e-cash? If it is a private agency like a bank, who will guarantee the safety of one's e-cash? Deposits in scheduled banks are normally insured by Reserve Bank (upto a specified limit).
- Will anonymity of e-cash transactions be ensured? Should it be ensured? (see *Box* 2).

Box 2: E-cash and Law Enforcement

Cash transactions ensure anonymity. It is the mode of payment to extortionists, corrupt officials and tax evaders. Large amounts of cash are bulky and difficult to transport and hide particularly because governments do not print high denomination currency notes. Currency is normally traceable with their serial numbers. Large amounts of cash are difficult to transport across national boundaries as customs officers keep a close watch. Ultimately the cash is deposited in a bank (for safety and to earn interest) and cash flow chokes. Except for very few countries banks are expected to provide information about deposits to law enforcement officials to prevent illegal transactions such as trade in narcotics. Electronic cash can cross national boundaries at lightning speed. Anonymous e-cash will be difficult to trace. If there is no limit set on e-cash transaction amount, large amounts can flow with ease and law enforcement officials will be unable to trace the money.Thus governments may ultimately set a limit (for example Rs.5000/-) on individual e-cash transaction.

Box 3: Seigniorage

The term seigniorage evolved from early history of money when kings (or seignior – a feudal lord) had the exclusive right to mint money. The difference between the cost of minting money and its face value is profit earned by the king and is called seigniorage. In modern economy the printing cost of currency notes is not very significant. Further, the requirement which once existed of having gold reserves equivalent to currency in circulation has been dispensed with. Thus the concept of seigniorage in a modern monetary system managed by governments is incongruous. This concept, however, becomes relevant in e-cash. E-cash can be sold to customers at face value. The interest which accrues between the time e-cash is sold and the time at which it is used (or encashed) and debited to the seller is the equivalent of seigniorage earned by an issuing bank. Unless there is enough e-cash 'minted' by a bank and kept in circulation this amount may not make up for the expenses incurred by the bank in servicing e-cash. (Debit cards work on a similar idea to recover cost).

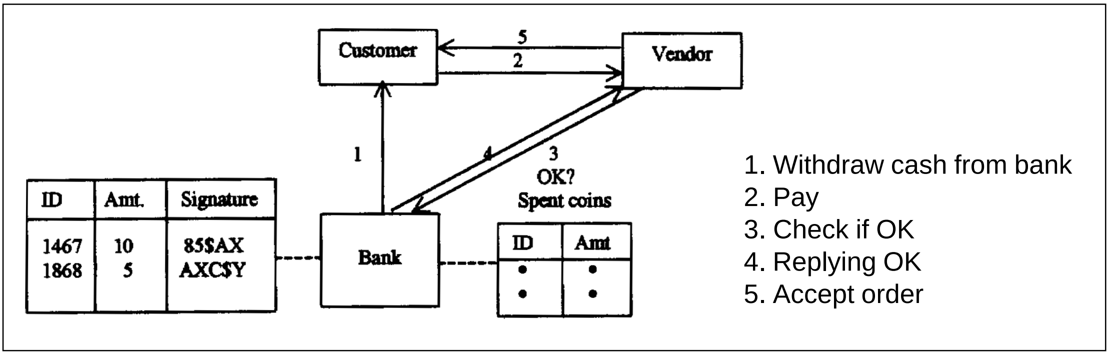
- Will e-cash issued by a private agency be universally acceptable? Can two individuals exchange e-cash without the issuing party entering into a transaction? (This is a major advantage of cash. I can borrow a hundred rupees from a friend without the Reserve Bank knowing it!)
- How will it be possible to detect forgery?
- A person who 'buys' e-cash should not be able to spend the same cash again. Once it is exchanged for a service it must lose its value or be taken out of circulation.
- How is the cost of handling e-cash recovered? In the case of physical cash not only was cost recovered but a profit made by what is known as seigniorage (See *Box* 3).

Currently the technology of cash transactions in e-commerce has not matured. Many competing systems are being tried out, each with its own advantages and disadvantages. Governments do not want to allow large cash transactions to take place electronically (see *Box* 2).

Governments do not want to allow large cash transactions to take place electronically.

E-cash Transactions

We will now describe a simple method which has been used for e-cash transactions. It is being used by some banks in the United States and Europe. No such system exists in India as of



ID	Amt.	Signature
1467	10	85$AX
1868	5	AXC$Y

ID	Amt
•	•
•	•

Figure 1. Electronic cash payment.

now. It is primarily intended for small cash transactions. The procedure is as follows (see *Figure* 1).

Step 1: A customer withdraws ‘cash’ in various denominations from the issuing bank (or financial institution) and stores it in his PC. The withdrawal takes place by the customer giving a unique identification number and denomination of each coin and requesting the bank to digitally sign it. The bank signs a coin by encrypting (id#, denomination > with its private key. The signed e-coins are of the form <id#, denomination, bank’s signature>.

Step 2: The customer pays a vendor for goods ordered using the signed e-coins.

Step 3: The vendor sends the e-coin to the issuing bank for authorization.

Step 4: The bank checks whether the e-coin is signed by it and whether it has not been already spent. If it is a valid e-coin, it OKs the transaction and credits the amount to the vendor’s account. It puts the e-coin details in a spent e-coin data base so that if the e-coin is presented again it can dishonour it.

The communications between customer, vendor and the bank are also encrypted as the internet is used. As the amounts involved are small, symmetric cryptography is used for these communications as it is faster. There are two points, which need clarification. The first is the cost of servicing e-coins. Normally

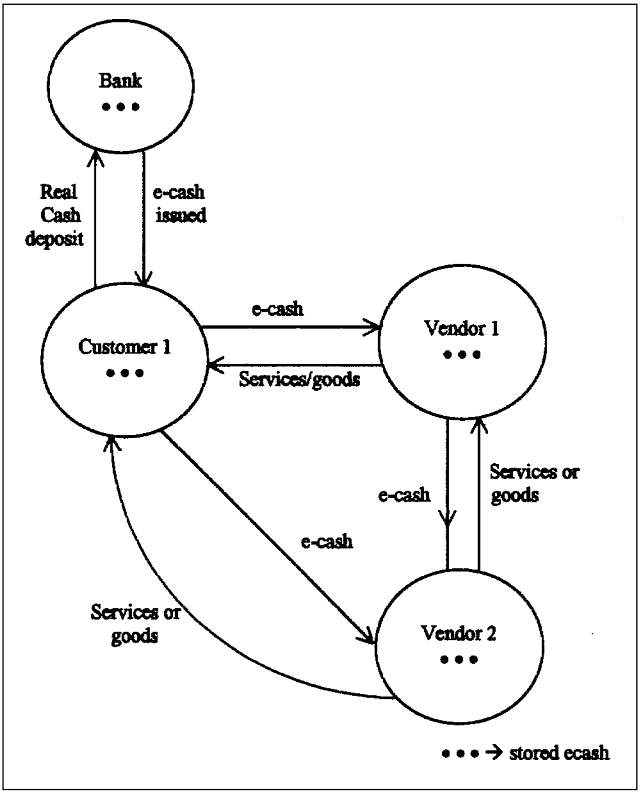


Figure 2. Circulation of e-cash.

banks will charge a small commission for the service from vendors. Second is whether a vendor who receives an e-coin from a customer can use it to purchase goods from another vendor. This is not possible as the issuing bank has to authenticate the e-coin and while doing it, it marks the coin as 'spent'. Thus it is not really like good old cash! To mimic real cash, e-cash should have features shown in *Figure* 2.

The sample protocol used above does not preserve the anonymity of cash. The bank will know which customer and vendor are involved in the cash transaction and can link the two. There is another protocol called transaction blinding in which it is possible for a customer to get e-coins issued by a bank without revealing his identity. The protocol called Chaum's blinding protocol is complicated, and as of now, not used widely. (Chaum invented the idea of blinding [2].)

Micro-payment for Information Goods

Micro-payment is a small payment of fractions of a rupee or a dollar when 'information goods' are delivered via the internet. By information goods we mean music files, video entertainment or text files (for example, works of fiction, software, technical information). Such a payment system is not yet in common use in India. It is being experimentally used in the United States and Europe. There are several competing systems. We will describe one such system called NetBill implemented by Carnegie Mellon University, Pittsburg, USA, in cooperation with Mellon Bank Corporation, Pittsburg.

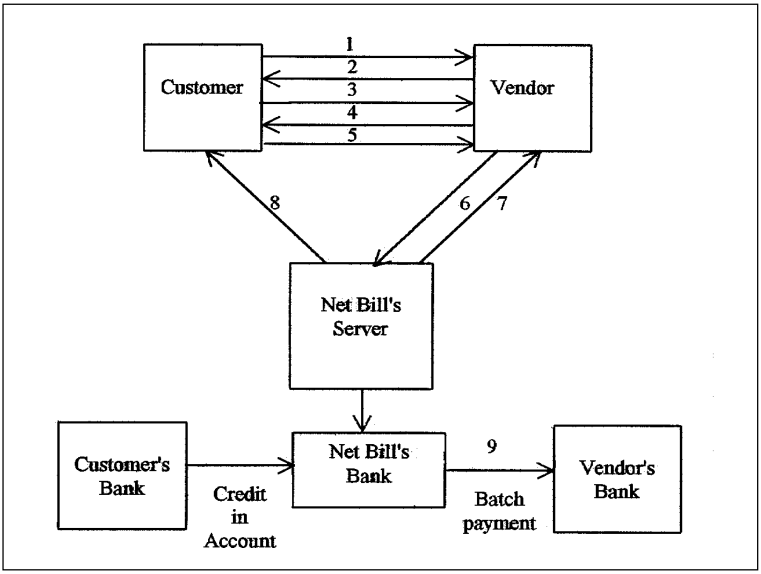


Figure 3. Micro-payments for information goods.

The main features of this payment system are:

1. The customer is charged only after the information is delivered.
2. The vendor is guaranteed payment when the information is delivered.
3. The customer deposits an amount which is debited when information is delivered to him. The payment system has nine steps described below (see also *Figure* 3).

Step 1: A customer requests a quote for 'information goods' from a vendor.
Step 2: Vendor sends a quote to the customer.
Step 3: The customer accepts the quote and notifies the vendor of acceptance.
Step 4: The vendor encrypts the information and sends it to the customer (note that the customer will require the key to decrypt the information).
Step 5: The customer sends a digitally signed payment order to the vendor consisting of the check sum of encrypted information received and the amount to be paid.
Step 6: The vendor verifies the payment order. If OK the key to decrypt the information, along with the payment order is digi-

tally signed and sent to the NetBill's server by the vendor.
Step 7: The Net Bill's server checks the customer's credit balance. If it is sufficient it debits his account based on the payment order. It credits the vendor's suspense account and sends an OK to the vendor.
Step 8: The Net Bill server sends the decryption key to the customer to enable him to decrypt the information received from the vendor.
Step 9. When the amount due to the vendor is substantial it is credited to his account by Net Bill.

Observe that in Step 4 the customer receives the information requested in encrypted form. It can be used by him only after payment is credited to vendor's account as the decryption key is sent only in Step 8. The checksum of information is deposited with Net Bill and in case of any dispute this provides the evidence of what actual information was delivered. Observe also that payments are consolidated and made to the vendor periodically. This is meant to reduce the transaction cost. The system is financed by charging a commission from the vendor.

We reiterate that electronic cash payments have not yet become mature. A number of issues need resolution before a universally accepted standard is evolved.

Suggested Reading

[1] Special issue, Electronic Money, *IEEE Spectrum*, Vol.34, No.2, February, 1997.

[2] D Chaum, Achieving Electronic Privacy, *Scientific American*, pp.96-101, August 1992.

[3] *Money: What it is and how it works,* http://wfhummel.cnchost.com/seignorage.html

[4] C Petrie, The Edge of E-Cash, *IEEE Internet Computing*, Vol.1, No.6, 1997.

[5] D C Lynch and L Lundquist, *Digital Money: The New Era of Internet Commerce,* John Wiley and Sons, New York, 1996.

Address for Correspondence
V Rajaraman
IBM Professor of Information Technology
JNCASR
Bangalore 560 064, India.
Email:rajaram@serc.iisc.ernet.in