ISSN 1512-1232

A NOVEL VIEW ON ELECTRONIC CASH AND ELECTRONIC PAYMENT SCHEMES: A COMPREHENSIVE STUDY

Dr.S.S.Riaz Ahamed

Principal, Sathak Institute of Technology, Ramanathapuram, Tamilnadu, India.
Email:ssriaz@ieee.org, ssriaz@yahoo.com

Abstract

Electronic payment systems are rapidly increasing in banking, retail, health cares, on-line markets, and even government - in fact, anywhere money needs to change hands. Organizations are motivated by the need to deliver products and services more cost effectively and to provide a higher quality of service to customers. Electronic payment systems are becoming central to on-line business process innovation as companies look for ways to serve customers faster and at lower cost. Emerging innovations in the payment for goods and services in electronic commerce promise to offer a wide range of new business opportunities. Electronic commerce is providing a facility for people to do on-line shopping and do business transactions electronically.

1.1 Introduction

Payment and settlement process is a potential bottleneck in the fast-moving electronic commerce environment if we rely on conventional payment methods such as cash, checks, bank drafts, or bills of exchange. Electronic replicas of these conventional instruments are not well suited for the speed required in e-commerce purchase processing. For instance, payments of small denominations (micropayments) must be made and accepted by vendors in real time for small amount of information. Conventional instruments are too slow for micropayments and the high transaction costs involved in processing them add greatly to the overhead. Therefore new methods of payment are needed to meet the emerging demands of e-commerce. These new payment instruments must be secure, have low processing cost, and be accepted widely.

The following issues need to be considered for designing a suitable electronic payment system.

- Form and characteristics of payment instruments - for example, electronic cash, electronic checks, credit/debit cards.
- The financial risks like privacy, fraud, mistakes, as well as other risks like bank failures associated with various payment instruments.
- Security features like authentication, privacy, and anonymity required to reduce these risks.
- The step-by-step procedures and institutional arrangements that form the fabric of the electronic payment business process that link consumers and organizations.

1.2 Types of Electronic Payment systems

Research into electronic payment systems for consumers can be traced back to the 1940s, and the first applications - credit cards - appeared soon after. In the early 1970s, the emerging electronic payment technology was labeled electronic funds transfer (EFT). EFT is defined as "any transfer of funds initiated through an electronic terminal, telephonic instruments, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account. " EFT utilizes computer and telecommunication components both to supply and to transfer money or financial assets. Transfer is information-based and intangible. Thus EFT stands in marked contrast to conventional money and payment modes that rely on physical delivery of cash or checks (or other paper orders to pay) by truck, train, or airplane.

Work on EFT can be segmented into three broad categories:

ISSN 1512-1232

- On-line electronic commerce payments
  - Token-based payment system
  - Electronic cash (e.g., DigiCash)
  - Electronic checks (e.g., NetCheque)
  - Smart cards or debit cards (e.g., Modex Electronic Currency Card)
- Credit cards-based payments systems
  - Encrypted credit cards (e.g., World Wide Web form-based encryption)
  - Third-party authorization numbers (e.g., First Virtual)

- Retailing payments
  - Credit cards (e.g., VISA or MasterCard)
  - Private label credit/debit cards (e.g., J.C. Penney Card)
  - Charges cards (e.g., American Express)

- Banking and financial payments
  - Large-scale or wholesale payments (e.g., bank-to-bank transfer)
  - Small-scale or retail payments (e.g., automated teller machines and cash dispensers)
  - Home banking (e.g., bill payment)

1.3 Online Electronic Commerce Payments

1.3.1 Digital Token-based Electronic Payment Systems

None of the banking or retailing payment methods are completely adequate in their present form for the consumer-oriented e-commerce environment. Their deficiency is their assumption that the parties will at some time or other be in each other's physical presence or that there will be a sufficient delay in the payment process for frauds, overdraft, and other undesirables to be identified and corrected. These assumptions may not hold for e-commerce and so many of these payment mechanisms are being modified and adapted for the conduct of business over networks.

Entirely new forms of financial instruments are also being developed. One such new financial instrument is "electronic tokens" in the form of electronic cash/money or checks. Electronic tokens are designed as electronic analogs of various forms of payment backed by a bank or financial institution. Simply stated, electronic tokens are equivalent to cash that is backed by a bank.

Electronics tokens are of three types:

1. Cash or real-time - Transactions are settled with the exchange of electronic currency. An example of on-line currency exchange is electronic cash (e-cash).
2. Debit of prepaid - Users pay in advance for the privilege of getting information. Examples of prepaid payment mechanisms are stored in smart cards and electronic purses that store electronic money.
3. Credit or postpaid - The server authenticates the customers and verifies with the bank that funds are adequate before purchase. Example of postpaid mechanisms is credit/debit cards and electronic checks.

The following points must be considered to understand the different viewpoints that these payment instruments bring to electronic commerce.

1. *The nature of the transaction for which the instrument is designed.* The tokens need to be specifically designed to handle various types of transactions like, payments for small pieces of information(micropayments), payments for more traditional products, specific transactions and more general transactions. The key is to identify the parties involved, the average amounts, and the purchase interaction.

ISSN 1512-1232

2. *The means of settlement used* - Tokens must be backed by cash, credit, electronic bill payments (prearranged and spontaneous), cashier's checks, IOUs, letters and lines of credit, and wire transfers, to name a few. Each option incurs trade-offs among transaction speed, risk, and cost. Most transaction settlement methods use credit cards, while others use other proxies for value, effectively creating currencies of dubious liquidity and with interesting tax, risk, and float implications.
3. *Approaches to security, anonymity, and authentication* - Electronic tokens vary in the protection of privacy and confidentiality of the transactions. Some may take care of privacy, while others may not. Encryption can help with authentication, nonrepudiability, and asset management.
4. *The question of risk* - The tokens might suddenly become worthless and the customers might have the currency that nobody will accept. If the system stores value in a smart card, consumers may be exposed to risk as they hold static assets. Also electronic tokens might be subject to discounting. Risk also arises if the transaction has long lag times between product delivery and payments to merchants. This exposes merchants to the risk the buyers don't pay - or vice - versa that the vendor doesn't deliver.

1.4 Internet Monetary Payment and Security Requirements

For consumers and merchants to be able to trust one another, prevent transmitted payment information from being tampered with, and complete transactions with any valid party, the following issues need to be addressed.

- Confidentiality of payment information
- Payment Information Integrity
- Account holder and merchant authentication
- interoperability

1. Confidentialiality of payment information

Payment information must be secure as it travels across the Internet without security, payment information could be picked up by hackers at the router, communication-line possibly resulting in the production of counterfeit cards of fraudulent transactions. To provide security, account information and payment information will need to be encrypted. This technology has been around for decades.

2. Payment Information Integrity

Payment information sent from consumers to merchants includes order information, personal data, and payment instructions. If any piece of the information is modified, the transaction may no longer be accurate. To eliminate this possible source of error or fraud, an arithmetic algorithm called hashing, along with the concept of digital signatures is employed. The hash algorithm generates a value that is unique to the payment information to be transferred. The value generated is calleda hash value ormessage diges. A helpul way to view a hash algorithm is as a one-way public cipher, in that:

- It has no secret key
- Given a message digest, there is no way to reproduce the original information
- It is impossible to hash other data with the same value.

To ensure integrity, the message digest is transmitted with the payment information. The receiver would then validate the message digest by recalculating it once payment information is received. If the message digest does not calculate to the same value sent, the payment information is assumed to corrupted and is therefore discarded. The hash algorithm, however, is public information; therefore, anyone may be able to alter the data and recalculate a new, “correct”

ISSN 1512-1232

message digest. To rectify this situation, the message digest is encrypted using a private key of the sender. This encryption of the message digest is called a digital signature.

Because a digital signature is created by using public-key cryptography, it is possible to identify the sender of the payment information. Since the encryption is done by using the private key of a public/private key pair, this means only the owner of that private key can encrypt the message digest. Therefore, if the decrypted digital signature equals the message digest calculated by the receiver, then the payment information could not have come from anyone but the owner of the private key.
Note that the roles of the public/private key pair in the digital signature process are the reverse of that used in ensuring information confidentiality. In the digital signature process, the private key is used to encrypt the information and the public key is used to decrypt.

3. Account holder and merchant authentication

Similar to the way card accounts are stolen and used today, it is possible for a person to use a stolen account and try to initiate an electronic commerce transaction. To protect against this a process that links valid account to a customer's digital signature needs to be established. A way to secure this link is by use of a trusted third party who could validate the public key and account of the customer. This third party could be one of many organizations, depending upon the type of account used.
In any instance, the best way for a third party to validate the public key and account is by issuing the items to the customer, together under the digital signature of the third party. Merchants would then decrypt the public key of the customer and, by definition of public-key cryptography, validate the public key and account of the customer. For the preceding to transpire, however, the following is assumed:

- The public key(s) of the third party(ies) is widely distributed.
- The public key(s) of the third party(ies) is highly trusted on face value.
- The third party(ies) issue public keys and accounts after receiving some proof of an individual's identity.

So far, it has been assumed that error or fraud takes place only on the customer end of payment information transport. However, the possibility exists that a fraud agent may try and pose as a merchant for a purpose of gathering account information to be used in a criminal manner in the future. To combat this fraud, the same third party process is used for merchants.

4. Interoperability

For electronic commerce to take place, customers must able to communicate with any merchant. For this reason, security and process standards must support any hardware or software platform that a customer or merchant may use and have no preferences over another. Interoperability is then achieved by using a particular set of publicly announced algorithms and processes in support of electronic commerce.

1.5 Payment and Purchase Order Process

For an electronic payment to occur over the internet, the following transactions/processes must occur

1. Account Holder Registration
2. Merchant Registration
3. Account holder ordering
4. Payment authorization

1. Account Holder Registration

ISSN 1512-1232

Account holders must register with a third party(TP) that corresponds to a particular account type before they transact with any merchant. In order to register, the account holder must have a copy of the TP's public key of the public/private key set. The manner in which the account holder receives the public key could be through various methods such as e-mail, Web-page download, disk, or flashcard. Once the account holder receives the public key of the TP, the registration process can start. Once the account holder's software has a copy of the TP's public key, the account holder can begin to register his or her account for Internet use. To register , the account holder will most likely be required to fill out a form requesting information such as name, address, account number, and other identifying personal information. When the form is completed, the account holder's software will do the following:

1. Create and attach the account holder's public key to the form
2. Generate a message digest from the information
3. Encrypt the information and message digest using a secret key
4. Encrypt the secret key using the TP's public key
5. Transmit all items to the TP.

When the TP receive the account holder's request, it does the following

1. Decrypts the secret key
2. Decrypts the information, message digest, and account holder's public key
3. Computes and compares message digests.

Assuming the message digests compute to the same value, the TP would continue the verification process using the account and personal information provided by the requesting account holder. It is assumed the TP would use its existing verification capabilities in processing in personal information. If the information in the registration is verified, the TP certifies the account holder's public key and other pertinent account information by digitally signing it with the TP's private key. The certified documentation is then encrypted using a secret key, which is in turn encrypted with the account holder's public key. The entire response is then transmitted to the customer.

Upon receipt of the TP's response, the account holder's software would do the necessary decryption to obtain the certified documentation. The certified documentation is then verified by the account holder by using the public key of the TP, thus checking digital signature. Once validated, the certified documentation would be held by the account holder's software for future use in electronic commerce transactions.

2. Merchant registration:

merchants must register with TPs that correspond to particular account types that they wish to honor before transacting business with customers who share the same account types. For example, if a merchant wishes to accept visa and mastercard, that merchant may have to register with tow TPs or find a TP that represents both. The merchant registration is similar to the account holder's registration process. Once merchant information is validated, certified documentation is transmitted to the merchant from the TP(s). the certified documentation is then stored on the merchant's computer for future use in electronic transactions.

3. Account holder (customer) ordering:

to send a message to a merchant the customer must have a copy of the merchant's public key and a copy of the TP's public key that corresponds to the account type to be used. The order process starts when the merchant sends a copy of its CD to the customer. At some point prior to sending the CD, the merchant must request the customer to specify what type of account will be used so that the appropriate CD will be sent. After receipt of the appropriate merchant CD, the customer software verifies the CD by applying the TP's public key, thus verifying the digital signature of the TP. The

ISSN 1512-1232

software then holds the merchant's CD to be used later in the ordering process. Once the order from is completed, the customer software does the following

- Encrypts account information with the TP's public key
- Attaches encrypted account information to the order form
- Creates a message digest of the order form and digitally signs it with the customer's private key.
- Encrypts the following with the secret key: order form
- Encrypts secret key with the merchatn's public key from the merchant's CD
- Transmits th esecret-key-encrypted message and encrypted secret key to the merchant

When the merchant software receives the order it does the following

- Decrypts the secret key using the private key of the merchant
- Decrypts the order form, digital signature, and customer's CD using the secret key
- Decrypts the message digest using the customer's public key obtained from the customer's CD
- Calculates the message diges from the order form and compares with the customer's decrypted message digest

4.payment authorization

during the processing of an order, the merchants will need to authorize the transaction with the TP responsible for that particular account. This authorization assures the merchant that the necessary funds or credit limit is available to cover the cost of the order. Also, note that the merchant has no access to the customer's account information since it was encrypted using the TP's public key; thus, it is required that this information be sent to the TP so that the merchant can receive payment authorization from the TP so that the merchant can receive payment authorization from the TP and that the proper customer account is debited for the transaction. It is assumed that the eventual fund transfer from some financial institution to the merchant and the debit transaction to the customer account takes place through an existing reestablished financial process.

It requesting payment authorization, the merchant software will send the TP the following information using encryption and the digital signature processes previously described:

- Merchant's CD
- Specific order information such as amount to be authorized, order number, date
- Customer's CD
- Customer's account information

After verifying the merchant, customer, and account information, the TP would then analyze the amount to be authorized. Should the amount meet some established criterion, the TP would send authorization information back to the merchant.

1.6 Electronic Cash (e-cash)

Cash is still the most prevalent and dominant form of consumer payment even after thirty years of continuous developments in electronic payment systems for three reasons:

- Lack of trust in the banking systems
- Inefficient clearing and settlement of non-cash transaction,
- Negative real interest rates paid on bank deposits.

To really displace cash, the electronic payment systems need to have some qualities of cash that current credit and debit cards lack. For example, *cash is negotiable*, meaning it can be given or traded to someone else. *Cash is legal tender*, meaning the payee is obligated to take it. *Cash is a bearer instrument*, meaning that possession is prima facie proof of ownership. Also, cash can be held and used by anyone even those who don't have a bank account, and cash places no risk on the part of the acceptor that the medium of exchange may not be good.

ISSN 1512-1232

Comparing cash to credit and debit cards, first, they *can't be given away* because, technically, they are identification cards owned by the issuer and restricted to one user. *Credit and debit cards are not legal tender*, given that merchants have the right to refuse to accept them. They *are not bearer instruments*; their usage requires an account relationship and authorization system. Similarly, checks require either personal knowledge of the payer or a check guarantee system. Hence, to really create a novel electronic payment method, we need to do more than recreate the convenience that is offered by credit and debit cards. We need to develop e-cash that has some of the properties of cash.

Electronic cash (e-cash) is a new concept in on-line payments systems because it combines computerized convenience with security and privacy that improve on paper cash. Its versatility opens up a host of new markets and applications. E-cash presents some interesting characteristics that should make it an attractive alternative for payment over the Internet. E-cash focuses on replacing cash as the principal payment mode in consumer-oriented electronic payments.

Properties of Electronic Cash

E-cash must have the following four properties: monetary value, interoperability, retrievability and security.

E-cash must have a monetary value; cash (currency), bank-authorized credit, or a bank-certified cashier's check must back it. When e-cash created by one bank, is accepted by others, reconciliation must occur without any problems. Stated another way, e-cash without proper bank certification carries the risk that when deposited, it might be returned for insufficient funds.

E-cash, must be interoperable - that is, exchangeable as payment for other e-cash, paper cash, goods or services, lines of credit, deposits in baking accounts, bank notes or obligations, electronic benefits transfers, and the like. Most e-cash proposals use a single bank. In practice, multiple banks are required with an international clearinghouse that handles the exchangeability issues because all customers are not going to be using the same bank or even be in the same country.

E-cash must be storable and retrievable. Remote storage and retrieval (e.g., from a telephone or personal communication device) would allow users to exchange e-cash from home or office or while traveling. The cash could be stored on a remote computer's memory, in smart cards, or in other easily transported standard or special-purpose devices. Because it might be easy to create counterfeit cash that is stored in a computer, it might be preferable to store cash on a dedicated device that cannot be altered. This device should have a suitable interface to facilitate personal authentication using passwords or other means and a display so that the user can view the card contents. One example of a device that can store e-cash is the Mondex card - a pocketsize electronic wallet.

E-cash should not be easy to copy or tamper with while being exchanged; this includes preventing or detecting duplication and double spending. Counterfeiting poses a particular problem, since a counterfeiter may, in the Internet environment, be anywhere in the world and consequently be difficult to catch without appropriate international agreements. Detection is essential in order to audit whether prevention is working. Then there is the tricky issue of double spending . For instance, you could use your e-cash simultaneously to buy something in Japan, India, and England. Preventing double spending from occurring is extremely difficult if multiple banks are involved in the transaction. For this reason, most systems rely on post-fact detection and punishment.

ISSN 1512-1232

Electronic Cash in Action

Electronic cash is based on cryptographic systems called "digital signatures". This method involves a pair of numeric keys (very large integers or numbers) that work in tandem: one for locking (or encoding) and the other for unlocking (or decoding). Messages encoded with one numeric key can only be decoded with the other numeric key and none other. The encoding key is kept private and the decoding key is made public.

By supplying all customers (buyers and sellers) with its public key, a bank enables customers to decode any message (or currency) encoded with the bank's private key. If decoding by a customer yields a recognizable message, the customer can be fairly confident that only the bank could have encoded it. These digital signatures are very secure and have proved over the past two decades to be more resistant to forgery than handwritten signatures. Before e-cash can be used to buy products or services, it must be procured from a currency server.

Purchasing E-cash from Currency servers

The purchase of e-cash from an on-line currency server (or bank) involves two steps:

- Establishment of an accounts and
- Maintaining enough money in the account to back the purchase. Some customers might prefer to purchase e-cash with paper currency, either to maintain anonymity or because they don't have a bank account.

Currently, in most e-cash trials all customers must have an account with a central on-line bank. This is overly restrictive for international use and multicurrency transactions for customers should be able to access and pay for foreign services as well as local services. To support this access, e-cash must be available in multiple currencies backed by several banks. A service provider in one country could then accept tokens of various currencies from users in may different countries, redeem them with their issuers, and have the funds transferred back to banks in the local country. A possible solution is to use an association of digital banks similar to organizations like VISA to serve as a clearinghouse for many credit card issuing banks.

And finally, consumers use the e-cash software on the computer to generate a random number, which serves as the "note". In exchange for money debited form the customer's account, the bank uses its private key to digitally sign the note for the amount requested and transmits the note back to the customers. The network currency server, in effect, is issuing a "bank note", with a serial number and a dollar amount. By digitally signing it, the bank is committing itself to back that note with its face value in real dollars.

This method of note generation is very secure, as neither the customer (payer) nor the merchant (payee) can counterfeit the bank's digital signature (analogous to the watermark in paper currency). Payer and payee can verify that the payment is valid, since each knows the bank's public key. The bank is protected against forgery, the payee against the bank's refusal to honor a legitimate note, and the user against false accusations and invasion of privacy.

untraceable currency. What makes it even more interesting is that users can prove unequivocally that they did or did not make a particular payment. This allows the bank to sign the "note" without ever actually knowing how the issued currency will be used.

Using the Digital Currency

Once the tokens are purchased, the e-cash software on the customer's PC stores digital money undersigned by a bank. The user can spend the digital money at any shop accepting e-cash, without having to open an account there first or having to transmit credit card numbers. As soon as the

ISSN 1512-1232

customer wants to make a payment, the software collects the necessary amount from the stored tokens.

Two types of transactions are possible: bilateral and trilateral. Typically, transactions involving cash are bilateral or two-party (buyer and seller) transactions, whereby the merchant checks the authenticity of the note's digital signature by using the bank's public key. If satisfied with the payment, the merchant stores the digital currency on his machine and deposits it later in the bank to redeem the face value of the note. Transactions involving financial instruments other than cash are usually trilateral or three-party (buyer, seller, and bank) transactions, whereby the "notes" are sent to the merchant, who immediately sends them directly to the digital bank. The bank verifies the validity of these "notes" and that they have not been spent before. The account of the merchant is credited. In this case, every "note" can be used only once.

In many business situations, the bilateral transaction is not feasible because of the potential for double spending, which is equivalent to bouncing a check. Double spending becomes possible because it is very easy to make copies of the e-cash, forcing banks and merchants to take extra precautions.

To uncover double spending, banks must compare the note passed to it by the merchant against a database of spent notes. Just as paper currency is identified with a unique serial number, digital cash can also be protected. The ability to detected double spending has to involve some form of registration so that all "notes" issued globally can be uniquely identified. However, this method of matching notes with a central registry has problems in the on-line world. For most systems, which handle high volumes of micropayments, this method would simply be too expensive. In addition., the problem of double spending means that banks have to carry added overhead because of the constant checking and auditing logs.

Double spending would not be a major problem if the need for anonymity were relaxed. In such situations, when the consumer is issued a bank note, it is issued to the person's unique license. When he or she gives it to some body else, it is transferred specifically to that other person's license. Each time the money changes hands, the old owner adds a tiny bit of information to the bank note based on the bank note's serial number and his or her license. If somebody attempts to spend money twice, the bank will now be able to use the two bank notes to determine who the cheater is. Even if the bank notes pass through many different people's hands, whoever cheated will get caught, and none of the other people will ever have to know. The downside is that the bank can tell precisely what your buying habits are since it can check the numbers on the e-cash and the various merchant account that are being credited. Many people would feel uncomfortable letting others know this personal information.

One drawback of e-cash is its inability to be easily divided into smaller amounts. It is often necessary to get small denomination change in business transactions. A number of variations have been developed for dealing with the "change" problem. For the bank to issue users with enough separate electronic "coins" of various denominations would be cumbersome in communication and storage. So would a method that required payees to return extra change. To sidestep such costs, customers are issued a single number called an "open check" that contains multiple denomination values sufficient for transaction up to a prescribed limit. At payment time, the e-cash software on the client's computer would create a not of the transaction value form the "open check".

ISSN 1512-1232

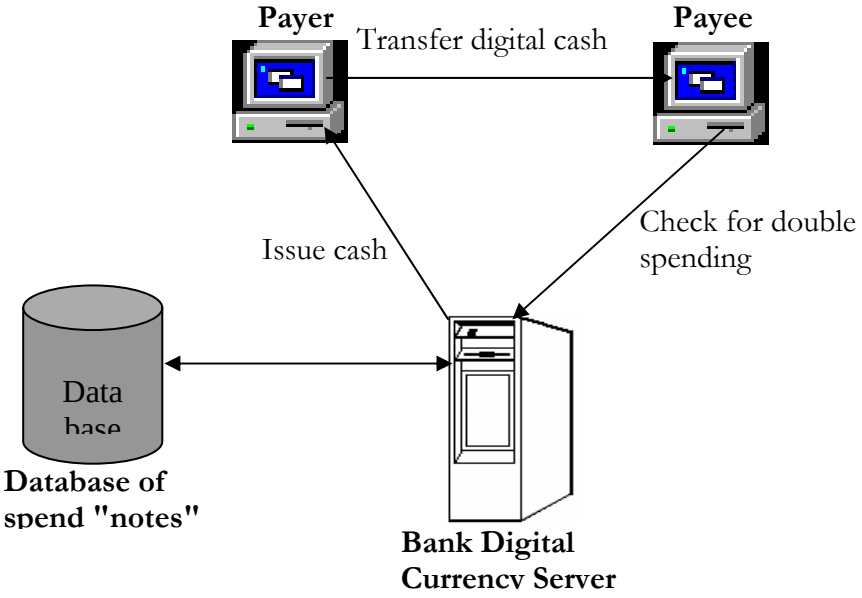

Fig Detection of double spending

Business issues and Electronic Cash

Electronic cash fulfills two main functions as a medium of exchange and as a store of value. Digital money is perfect medium of exchange. By moving monetary claims quickly and by effecting instant settlement of transaction, e-cash may help simplify the complex interlocking credit and liabilities that characterize today's commerce. For instance, small businesses that spend month waiting for big customers to pay their bills would benefit hugely from a digital system in which instant settlement is the norm.

The controversial aspects of e-cash are those that relate to the other role, as a store of value. Human needs tend to require that money take tangible form and be widely accepted, or "legal tender". The enormous currency fluctuations in international finance pose another problem. On the Internet, the buyer could be in Mexico and the seller in the United States. How do you check that the party in Mexico is giving a valid electronic currency that has suitable backing? Even if it were valid today, what would happen if a sudden devaluation occurs overnight.

From a banker's point of view, e-cash would be a mixed blessing. Because they could not create new money via leading in the digital world, banks would see electronic money as unproductive. They might charge for converting it, or take a transaction fee for issuing it, but on-line competition would surely make this a low-profit affair. In the short term, banks would probably make less from this new business than they would lose from the drift of customers away from traditional services. It seems unlikely that e-cash would be allowed to realize its potential for bypassing /the transaction costs of the foreign-exchange market.

Operational Risk and Electronic Cash

Operational risk associated with e-cash can be mitigated by imposing constraints, such as limits on

1. the time over which a given electronic money is valid,
2. how much can be stored on and transferred by electronic money,
3. the number of exchanges that can take place before a money needs to be re-deposited with a bank or financial institution, and
4. the number of such transactions that can be made during a given period of time.

ISSN 1512-1232

The objective of imposing constraints is to limit the issuer's liability. A maximum upper limit could be imposed on the value that could be assigned to any single transaction or that could be transferred to the same vendor within a given period of time.

Legal Issues and Electronic Cash

Electronic cash will force bankers and regulators to make though choices that will shape the form of lawful commercial activity related to electronic commerce. As result of the very features that make it so attractive to many, cash has occupied an unstable and uncomfortable place within the existing taxation and law enforcement systems.

Anonymous and virtually untraceable, cash transactions today occupy a place in a kind of underground economy. This underground economy is generally confined to relatively small-scale transactions because paper money in large quantities is cumbersome to use and manipulate-organized crime being the obvious exception. As long as the transactions are small in monetary value, the government tolerates them as an unfortunate but largely insignificant by-product of the modern commercial state. As transactions get larger the government becomes more suspicious and enlists the aid of the banks, through the various currency reporting laws, in reporting large disbursements of cash so that additional oversight can be ordered.

Electronic checks

Electronic checks are another form of electronic tokens. They are designed to accommodate the many individuals and entities that might prefer to pay on credit or through some mechanism other than cash. In the model shown in figure, buyers must register with a third-party account server before they are able to write electronic checks. The account server also acts as a billing service. The registration procedure can vary depending on the particular account server and may require a credit card or a bank account to back the checks.

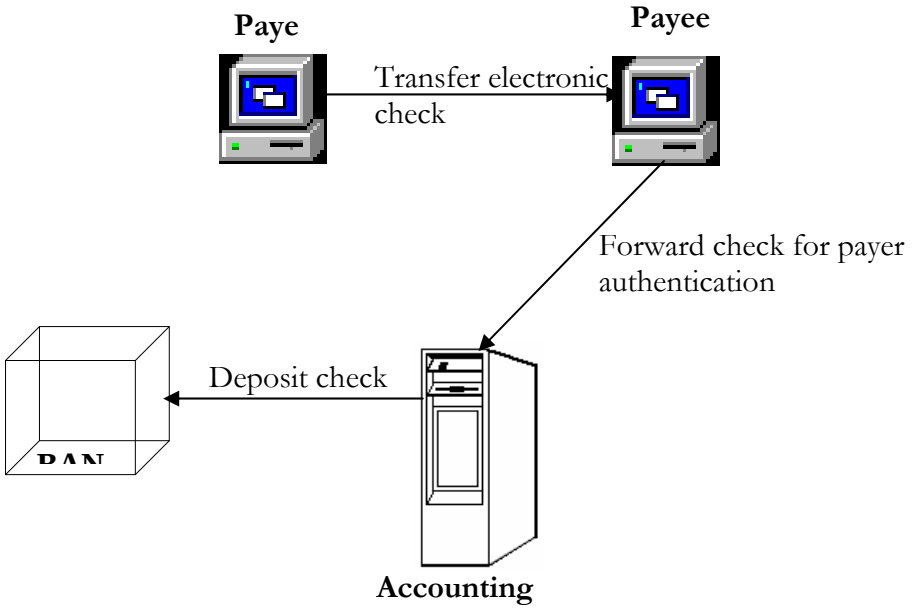

Fig. Payment transaction sequence in an electronic check

Once registered, a buyer can then contact sellers of goods and services. To complete a transaction, the buyer sends a check to the seller for a certain amount of money. These checks may be sent using e-mail or other transport methods. When deposited, the check authorizes the transfer of account balances from the account against which the check was drawn to the account to which the check was deposited.

ISSN 1512-1232

The specifics of the technology work in the following manner: On receiving the check, the seller presents it to the accounting server for verification and payment. The accounting server verifies the digital signature on the check using the Kerberos authentication scheme. In the language of Kerberos, an electronic check is a specialized kind of "ticket" created by the Kerberos system. A user's digital "signature" is used to create one ticket - a check - which the seller's digital "endorsement" transforms into another - an order to a bank computer for fund transfer. Subsequent endorsers add successive layers of information onto the tickets, precisely as large number of banks may wind up stamping the back of a check along its journey through the system.

Electronic checks have the following advantages:

- They work in the same way as traditional checks, thus simplifying customer education.
- Electronic checks are well suited for clearing micropayments; their use of conventional cryptography makes it much faster than systems based on public-key cryptography (e-cash).
- Electronic checks create float and the availability of float is an important requirement for commerce. The third-party accounting server can make money by charging the buyer or seller a transaction fee or a flat rate fee, or it can act as a bank and provide deposit accounts and make money on the deposit account pool.
- Financial risk is assumed by the accounting server and may result in easier acceptance. Using multiple accounting servers provides reliability and scalability. There can be an inter-account server protocol to allow buyer and seller to "belong" to different domains, regions, or countries.

Smart Cards and Electronic Payment Systems

The enormous potential of electronic tokens is currently stunted by the lack of a widely accepted and secure means of transferring money on-line. In spite of the many prototypes developed, we are long way from a universal payment system because merchants and banks have to be signed up and a means has to be developed to transfer money. Such a system moreover must be robust and capable of handling a large number of transactions and will require extensive testing and usage to trap all the bugs.

In the meantime, thousands of would-be sellers of electronic commerce services have to pay one another and are actively looking for payment substitutes. One such substitute is the smart card. Smart cards have been in existence since the early 1980s and hold promise for secure transaction using existing infrastructure. Smart cards are credit and debit cards and other card products enhanced with microprocessors capable of holding more information than the traditional magnetic stripe. The chip, at its current state of development, can store significantly greater amounts of data, estimated to be 80 times more than a magnetic stripe.

Smart cards are basically of two types: relationship-based smart credit cards and electronic purses. Electronic purses, which replace money, are also known as debit cards and electronic money.

Relationship-Based Smart Cards

A relationship-based smart card is an enhancement of existing card services and/or the addition of new services that a financial institution delivers to its customers via a chip-based card or other device. These new services may include access to multiple financial accounts, value-added marketing programs, or other information cardholders may want to store on their card. The chip-

ISSN 1512-1232

based card is but one tool that will help alter mass marketing techniques to address each individual's specific financial and personal requirements. Enhanced credit cards store cardholder information including name, birth date, personal shopping preferences, and actual purchase records. This information will enable merchants to accurately track consumer behavior and develop promotional programs designed to increase shopper loyalty.

Relationship-based products are expected to offer consumers far greater options, including the following:

- Access to multiple accounts, such as debit, credit, investments or stored value for e-cash, on one card or an electronic device
- A variety of functions, such as cash access, bill payment, balance inquiry, of funds transfer for selected accounts.
- Multiple access options at multiple locations using multiple device types, such as an automated teller machine, a screen-phone, a personal computer, a personal digital assistant (PDA), or interactive TVs.

Electronic Purses and Debit Cards

Despite their increasing flexibility, relationship-based cards are credit based and settlement occurs at the end of the billing cycle. There remains a need for a financial instrument to replace cash. To meet this need, banks, credit card companies, and even government institutions are arching to introduce 'electronic purses", wallet-sized smart cards embedded with programmable microchips that store sums of money for people to use instead of cash for everything form buying food, to making photocopies, to paying subway fares.

The electronic purse works in the following manner. After the purse is loaded with money, at an ATM or through the use of an inexpensive special telephone, it can be used to pay for, say, candy in a vending machine equipped with a card reader. The vending machine need only verify that a card is authentic and there is enough money available for a chocolate bar. In one second, the value of the purchase is deducted form the balanced on the card and added to an e-cash box in the vending machine. The remaining balance on the card is displayed by the vending machine or can be checked at an ATM or with a balance-reading device. Electronic purses would virtually eliminate fumbling for change or small bills in a busy store or rush-hour toll both, and waiting for a credit card purchase to be approved. This allows customers to pay for rides and calls with a prepaid card that makes note of each transaction.

When the balance on an electronic purse is depleted, the purse can be arranged with more money. As for the vendor, the receipts can be collected periodically in person-or, more likely, by telephone and transferred to a bank account. While the technology has been available for a decade, the cards have been relatively expensive.

Smart-Card Readers and Smart phones

The smart-card reader features a two-line by 16-character display that can show both a prompt and the response entered by the user. Efficiency is further enhanced by colour-coded function keys, which can be programmed to perform the most frequently used operations in a single key-stroke. It can communicate via an RS-232 serial interface with the full range of transaction automation systems, including PCs and electronic cash registers (ECRs). Card readers in the form of screen phones are becoming more prominent.

Many bankers feel that screen-based phones are more convenient to use than PC-based home banking applications, which require users to boot up their systems and establish a modem

ISSN 1512-1232

connection before conducting transactions. Other features of screen phones include advanced telephone functions such as a two-way speaker phone capability, a dialing directory, and a phone log for tracking calls. Several financial institutions have teamed up with local companies in an effort to use these functions as a marketing tool for screen phones. Another feature of smart card readers is that they can be customized for specific environments.

Business Issues and Smart Cards

For merchants, smart cards are a very convenient alternative to handling cash, which is becoming a nightmare. Cash is expensive to handle, count, and deposit and incurs slippage, a commercial term for theft, fraud, or misplacement. Long-range planners in the banking industry see the weaning of small businesses and consumers from cash as the last step to closing many expensive branches and conducting virtually all business by telephone, through cash machines and perhaps home computers.

1.7 Credit Card-Based Electronic payment system

To avoid the complexity associated with digital cash and electronic checks, consumers and vendors are also looking at credit card payments on the Internet as one possible time-tested alternative. There is nothing new in the basic process. If consumers want to purchase a product or service, they simply send their credit card details to the service provider involved and the credit card organization will handle this payment like any other.

We can break credit card payment on on-line networks into three basic categories;

- Payments using plain credit card details
  The easiest method of payment is the exchange of unencrypted credit cards over a public network such as telephone lines or the Internet. The low level of security inherent in the design of the Internet makes this method problematic (any snooper can read a credit card number, and programs can be created to scan the Internet traffic for credit card numbers and send the numbers to its master). Authentication is also a significant problem, and the vendor is usually responsible to ensure that the person using the credit card is its owner. Without encryption there is no way to do this.

- Payments using encrypted credit card details
  It would make sense to encrypt your credit cards details before sending them out, but even then there are certain factors to consider. One would be the cost of a credit card transaction itself. Such cost would prohibit low-value payments (micropayments) by adding costs to the transactions.

- Payment using third-party verification
  One solution to security and verification problems is the introduction of a third party: a company that collects and approves payments from one client to another. After a certain period of time, one credit card transaction for the total accumulated amount is completed.

Encryption and Credit Cards

Encryption is instantiated when credit card information is entered into a browser or other electronic commerce device and sent securely over the network from buyer to seller as an encrypted message. To make a credit card transaction truly secure and nonrefutable, the following sequence of steps must occur before actual goods, services, or funds flow:

1. A customer presents his or her credit card information (along with an authenticity signature or other information such as mother's maiden name) securely to the merchant.
2. The merchant validates the customer's identity as the owner of the credit card account.

ISSN 1512-1232

3. The merchant relays the credit card charge information and signature to its bank or on-line credit card processors.
4. The bank or processing party relays the information to the customer's bank for authorization approval.
5. The customer's bank returns the credit card data, charge authentication, and authorization to the merchant.

In this scheme, each consumer and each vendor generates a public key and a secret key. The public key is sent to the credit card company and put on its public key server. The secret key is re-encrypted with a password, and the unencrypted version is erased. To steal a credit card, a thief would have to get access to both a consumer's encrypted secret key and password. The credit card company sends the consumer a credit card number and a credit limit. to buy something from vendor X, the consumer sends vendor X the message, "It is now time T. I am paying Y dollars to X for item Z," then the consumer uses his or her password to sign the message with the public key. The vendor will then sign the message with its own secret key and send it to the credit card, company, which will bill the consumer for Y dollars and give the same amount (less a fee) to X.

Nobody can cheat this system. The consumer can't claim that he didn't agree to the transaction, because he signed it. The vendor can't invent fake charges, because he doesn't have access to the consumer's key. He can't submit the same charge twice, because the consumer included the precise time in the message. To become useful, credit card systems will have to develop distributed key servers and card checkers. Otherwise, a concentrated attack on these sites could bring the system to a halt.

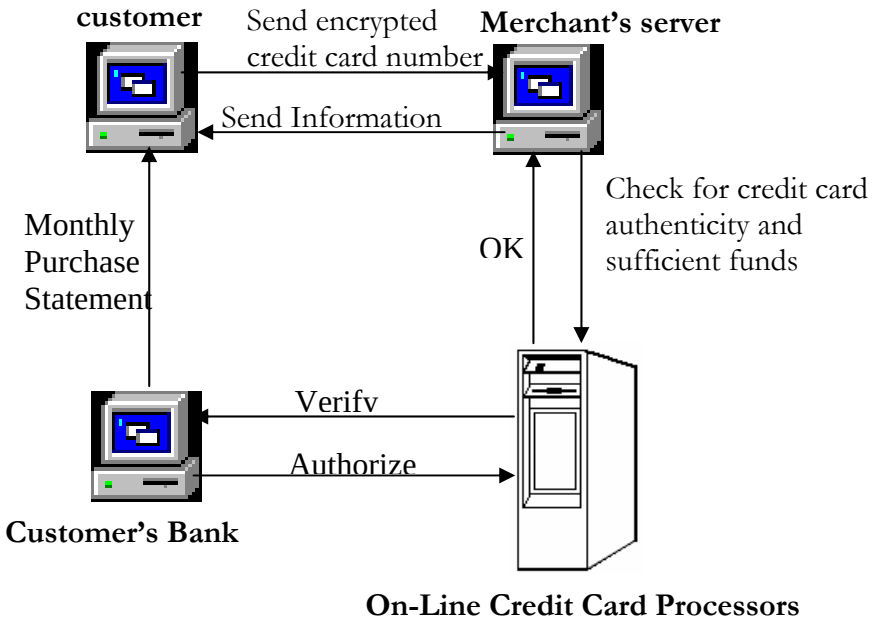

Fig Processing payments using encrypted credit cards

Third-Party Processors and Credit Cards

In third-party processing, consumers register with a third party on the Internet to verify electronic microtransactions. Verification mechanisms can be designed with many of the attributes of electronic tokens, including anonymity. They differ from electronic token systems in that (1) they depend on existing financial instruments and (2) they require the on-line involvement of at least one additional party and, in some cases, multiple parties to ensure extra security. However, requiring an on-line third-party connection for each transaction to different banks could lead to processing bottlenecks that could undermine the goal of reliable use.

ISSN 1512-1232

Examples of companies that are already providing third-party payment services on the Internet are First Virtual and Open Market. They are referred to as on-line third-party processors (OTPPs) since both methods are fairly similar in nature.

OTPPs have created a six-step process that they believe will be a fast and efficient way to buy information on-line:

1. The consumer acquires n OTPP account number by filling out a registration form. This will give the OTPP a customer information profile that is backed by a traditional financial instrument such as a credit card.
2. To purchase an article, software, or other information on-line, the consumer requests the item from the merchant by quoting her OTPP account number. The purchase can take place in one of two ways. The consumer can automatically authorize the "merchant" via browser settings to access her OTPP account and bill her, or she can type in the account information.
3. The merchant contacts the OTPP payment server with the customer's account number.
4. The OTPP payment server verifies the customer's account number for the vendor and checks for sufficient funds.
5. The OTPP payment server sends an electronic message to the buyers. This message could be an automatic WWW form that is sent by the OTPP server or could be a simple e-mail. The buyer responds to the form or e-mail in one three ways: yes, I agree to pay; No, I will not pay; or Fraud, I never asked for this.
6. If the OTPP payment server gets a Yes from the customer, the merchant is informed and the customer is allowed to download the material immediately.
7. The OTPP will not debit the buyer's account until it receives confirmation of purchase completion. Abuse by buyers who receive information or a product and decline to pay can result in account suspension.
8. To use this system, both customers and merchants must be registered with the OTPP.

Business Pros and Cons of Credit Card-Based Payment

Credit cards have advantages over checks in that the credit card company assumes a larger share of financial risk for both buyer and seller in a transaction. Buyers can sometimes dispute a charge retroactively and have the credit card company act on their behalf. Sellers are ensured that they will be paid for all their sales--they needn't worry about fraud. This translates into a convenience for the buyer, in the credit card transactions are usually quicker and easier than check (and sometimes even cash) transaction. One disadvantage to credit cards is that their transactions are not anonymous, and credit card companies do in fact compile valuable data about spending habits. Encryption and transaction speed must be balanced, however, as research has shown that on-line users get very impatient and typically wit for 20 seconds before pursuing other actions. Hence, on-line credit card users must find the process to be accessible, simple, and fast. Speed will have design and cost implications, as it is a function of network capabilities, computing power, available at every server, and the specific form of the transaction. The infrastructure supporting the exchange must be reliable. The user must feel confident that the supporting payment infrastructure will be available on demand and that the system will operate reasonably well regardless of component failures or system load conditions.

1.8 Conclusion

Electronic payment systems and e-commerce are intricately linked given that on-line consumers must pay for products and services. Clearly, payment is an integral part of the mercantile process and prompt payment (or account settlement) is crucial. If the claims and debit of the various participants -- individuals, companies, banks, and non-banks -- are not balanced because

ISSN 1512-1232

of payment delay or, even worse default, then the entire business chain is disrupted. Hence an important aspect of e-commerce is prompt and secure payment, clearing, and settlement of credit or debit claims.

1.9 References

1) Arnold, V. 2006. Behavioral research opportunities: Understanding the impact of enterprise systems. International Journal of Accounting Information Systems 7(1): 7-17.
2) Interactive Advertising Bureau. 2005. Interactive Advertising Basics 2005: 28 Reasons to Use Interactive Advertising.
3) Reid, Robert H. (1997). Architects of the Web: 1,000 Days that Built the Future of Business. John Wiley & Sons. Chapter Seven: 'Hotwired - Publishing on the Web' (pp 300-308) ISBN 0471171875
4) Strauss, J. and F. Raymond. 1999. Marketing on the Internet: Principles of Online Marketing. New Jersey: Prentice Hall Inc.
5) Kleindl, B. 2003. Strategic Electronic Marketing: Managing E-Business, 2e. South-Western Educational Publishing.
6) McCue, S. 2004. *Building E-Commerce Strategies: From Farce to Force*. South-Western Educational Publishing.
7) Davis, J. 2000. A Guide to Web Marketing: Successful Promotion on the Net. UK: Kogan Page Limited. ISBN 0749431857
8) Deise, M. V., C. Nowikow, P. King and A. Wright. 2000. Executive's Guide to E-Business: From Tactics To Strategy. John Wiley & Sons.
9) McCreary, L. 2008. What was privacy? *Harvard Business Review* (October): 123-131.
10) Chapman, Merrill R., In search of stupidity: over 20 years of high-tech marketing disasters (2nd Edition) , Apress, ISBN 1-59059-721-4
11) Janal, D. S. 1995. Online Marketing Handbook. New York: Van Nostrand Reinhold. ISBN: 0442020589
12) Sheehy, D. E. 2002. Discussion of An experimental examination of alternative forms of web assurance for business-to-consumer e-commerce. Journal of Information Systems (Spring Supplement): 55-57.
13) Shields, M. G. 2001. E-Business and ERP: Rapid Implementation and Project Planning. John Wiley & Sons.
14) Anderson, P. and E. Anderson. 2002. The new e-commerce intermediaries. MIT Sloan Management Review: 53-62.
15) Anthony, J. H., W. Choi and S. Grabski. 2006. Market reaction to e-commerce impairments evidenced by website outages. International Journal of Accounting Information Systems 7(2): 60-78.
16) Cronin, M. J. 2000. Unchained Value: The New Logic of Digital Business. Harvard Business School Press.
17) David, J. S. 2003. Discussion of Information transfer among internet firms: The case of hacker attacks. Journal of Information Systems : 83-86.
18) Deak, E. J. 2004. Economics of E-Commerce and the Internet with Economic Applications Card. South-Western Educational Publishing.
19) Knapp, M. 2003. E-Commerce: Real Issues and Cases. South-Western Educational Publishing.
20) Memp, P. 2006. Avatar-based marketing. Harvard Business Review (June): 48-57.
21) Mensah, N. and L. Velocci. 2006. Market reaction to e-commerce impairments evidenced by website outages: Discussant comments. International Journal of Accounting Information Systems 7(2): 82-86.
22) Miller, D. 2001. Rod Hoover: Royal & Sun Alliance sheds light on e-business and the state of insurance. Strategic Finance (March): 44-47.

ISSN 1512-1232

23) Monahan, S. J. 2002. Discussion of The value relevance of revenue for internet firms: Does reporting grossed-up or barter revenue make a difference? Studies on Accounting, Entrepreneurship and E-Commerce. Journal of Accounting Research: 479-484.
24) Mooney, J. L. and W. D. Pittman. 1996. A guide to electronic commerce. Management Accounting (September): 43-47.
25) Cucuzza, T. G. and J. Cherian. 2001. The internet and e-business: Trends and implications for the finance function. Journal of Cost Management (May/June): 5-14.
26) Daigle, R. J. 2004. Discussion of: SportsStuff.com: A case study of XML technologies, e-business processes, and accounting information systems. Journal of Information Systems: 75-77.
27) Dalton, D. 1999. Is e-business for you? Strategic Finance (March): 74-77.
28) Anthony, J. H., W. Choi and S. V. Grabski. 2006. Market reaction to e-commerce impairments evidenced by website outages authors' response. International Journal of Accounting Information Systems 7(2): 87-90.
29) Murthy, U. S. and S. M. Groomer. 2004. A continuous auditing web services (CAWS) model for XML-based accounting systems. International Journal of Accounting Information Systems (5): 139-163.
30) Murthy, U. S. and S. M. Groomer. 2004. Reply to the discussions of ‘A continuous auditing web services (CAWS) model for XML-based accounting systems’. International Journal of Accounting Information Systems (5): 175-181.
31) Norris, G., J. R. Hurley, J. Dunleavy and J. Balls. 2000. E-Business and ERP: Transforming the Enterprise. John Wiley & Sons.
32) O'Donnell, E. 2006. Discussion of the influence of scope and timing of reliability assurance in B2B E-Commerce. International Journal of Accounting Information Systems 7(2): 130-133.

Article received: 2010-04-12