ELECTRONIC PAYMENT SYSTEMS

A Survey Report submitted in partial fulfillment of the requirements of CMPE 296U

By

Srivalli Arkalgud
Student ID: 615906587

Prof Dr. Jerry Gao
Abstract

Electronic Commerce industry is exploding at a fast pace. One of the key aspects of electronic commerce is payments. There are different methods to pay electronically. These can be through Credit Cards, Electronic Checks, Electronic Cash, Debit Cards, or Charge Cards.

This paper discusses the major electronic payment methods namely Credit Card Processing, Electronic Check Processing, and Electronic Cash. It presents an overview of each architecture, and describes two commercial implementations of the architecture. The paper also analyses and compares the payment methods and reveals their advantages and disadvantages.
List of Figures

Figure 3.1: Entities in Conventional Credit Card Processing System

Figure 3.2: Authorization with First Data [9]

Figure 3.3: Capture/Settlement Process with First Data [9]

Figure 3.4: Buying with First Virtual [3]

Figure 3.5: CyberCash Model

Figure 4.1 NetBill Processing [7]
Table of Contents

Abstract
List of Figures
List of Tables

Introduction ........................................................................................................... 5
Motivation for E-Commerce ............................................................................... 7
Credit Card Payment System ........................................................................... 9
Electronic Check Payment System ................................................................. 19
Electronic Cash Payment System .................................................................. 25
Analysis and Comparison of Payment Systems .............................................. 29
Future of Electronic Payment Systems ............................................................ 36
References .......................................................................................................... 37
1. Introduction

Commerce is the most major aspect of any civilization. Improving Commerce can bring prosperity into all segments of society. In today's world there has been major changes to the commerce industry. The most important of it is the introduction of computers into the commerce industry. Computerization of commerce has taken the world by a storm. There are significant improvements in the areas of initiating sale of products, placing orders, making payments, and transfer of funds. This has led to a much better global economy and better living standards for all.

Payment started with the barter system centuries ago. Goods were exchanged directly between people in the barter system. The major draw back of barter system was that the buyer and the seller had to mutually like the goods that they had in surplus. This led to next generation of payment method called Commodity Money System. Here, the buyer would buy goods from the seller in exchange of some commodity in the form of gold, silver, corn etc. Commodity Money slowly evolved into standard of having paper notes at the exchange parameter. The cash payment method does not require the seller to like the commodity that he/she is going to receive in exchange for the goods. About 80 percent of all the transactions in the world are done through cash payment. The process is simple and there is no bank involvement. There is however an overhead of printing notes. The cash payment method is very insecure. There is no record of the transaction maintained. There is a possibility for generating counterfeit notes. Cash Payment is mostly used for low-value payments. Check Payment is employed for making medium to high value payment. A record of the transaction is maintained at the bank at the cost of the transaction fee. However, it is not a guaranteed form of payment since the checks do no represent real time cash. There is a possibility that the checks could be turned down by the buyer's bank due to various reasons. As the volume of check processing started increasing, banks had to think about ways of improving the turn-around time for payment processing.
Electronic Commerce is defined as a monetary transaction that occurs electronically as opposed to the physical exchange of money or checks. Tangible currency is eliminated and accounts are maintained electronically to reflect the effects of transaction. E-Commerce involves trading using the latest electronic equipment and software between the sellers and the buyers. The trade in e-commerce is conducted in a slightly different way than the traditional trading. The earliest form of automation in the financial industry was done to automate the functions of clearing house in bank associations. In 1968, group of California Bankers formed Special Committee on Paperless Entries (SCOPE) which led to the formation in 1972 of California Clearing House Association. This was the first regional automated Clearing House. The first form of automated payments was to disburse salaries to employees from an employer's account. Gradually, the information revolution changed the outlook of the banking sector and computerized majority of the functions. This led development of new forms of payment using the latest technology.

Electronic Payments can be categorized as Stored Account Payments or Stored Value Payments. In a stored account payment, the buyer and the merchant maintain accounts with a bank. The transactions are registered and the actual transfer of funds takes place at a later stage through settlement. Examples of Stored Account payment System include Credit Cards, Debit Cards and Electronic Checks. In Stored Value Payment System like smart cards, mondex cards, digital cash, certain amount of prepaid monetary value stored electronically on the card. Electronic Checks are also processes on the lines of traditional check processing. Each of these cards can have different ways.

The paper describes the various methods of making payments. Chapter 3 details Credit Card Payment System. Chapter 4 describes making payment using Electronic Checks. Chapter 5 outlines stored value systems like digital cash (eCash), and Smart Cards.
2. Motivation for Electronic Payments

Internet is growing at an extremely fast pace. It has been estimated that there is a new web page every minute. The ease of use, efficiency and quickness, search engines and international presence of Internet has been drawing millions of users towards it. The number of Internet users is expected to be 175 million by 2001. There has been 9 billion sales on the Internet in 1998. America Online stated that the sales for the six-week holiday season were 1.2 billion on its network alone. Expectations are that online sales will continue to rise. It has been estimated that Internet sales will grow to 18.2 billion in 1999, doubling its previous year's mark. As the number of Internet sales increases, more and more merchants are showing an interest in reaching customers through the Web.

The vast market opportunity on the Web means a challenging atmosphere to software engineers who work behind the screen to make things happen on the Web. With the exploding E-Commerce market, the E-Commerce software needs to process the transactions efficiently, more securely and with lesser communication delays.

Payment is the most vital aspect of a trade. Payment processing involves a development of complex, secure software for transferring financial data between the buyer, seller and the banking network. The loss from insecure payment systems amounted to nearly $250 million last year. Hence it becomes important to research into the providing a more stable and secure payment system for our exploding Internet economy.

The payment information contains private financial data that should be transferred using the most secure methodologies. The paper also discusses the various methods employed to incorporate security into electronic payment systems. Communication between trading partners called buyers and sellers are done using specific protocols called payment protocols.
There are various methods to implement electronic payment processing. However it is not clear as to which one will be the leader in the next 10 years. Hence it is very interesting to investigate the software growth and research that has been done in this area and develop more efficient and better software. The most popular payment method adopted in the US is credit card payment system. This payment method is studied in detail in the next chapter. Cashless (or rather noteless) society is envisaged by the usage of stored value payment methods. Two such methods called Electronic Check processing and Digital Cash are detailed in Chapter 4 and Chapter 5. Each of the payment methods are followed by a case study of a commercial product that offers that payment method.
3. Credit Card Payment System

Credit cards are payment cards issued by a bank against a special purpose account associated with some form of installment based re-payment scheme or revolving credit. [3]. This is also know as "Pay Later" method of payment. Diner's Club introduced the first credit card in 1958, followed by American Express in 1966. There are two major organizations issuing 80% of the credit cards in the market today. They are Visa International and MasterCard. These companies are made up of a larger number of member banks.

3.1 Overview

An overview of the credit card processing is depicted in the following diagram:

![Diagram of Credit Card Processing System](image-url)

*Figure 3.1: Entities in Conventional Credit Card Processing System*
There are four main partners in a Credit Card transaction. The Issuing Bank is the bank that maintains the account of the buyer and issues a Credit Card to the buyer. The issuing bank also sets a limit on the amount of purchases that can be made using the card and the percentage of interest on the unpaid portion of the bill. The cardholder is also known as the buyer in the transaction. The cardholder initiates a transaction. The merchant is the seller of goods and services. The merchant maintains an account with a bank or a financial institution known as the acquirer. Acquiring institutions contracts with merchants to enable them to accept credit card transactions and charges a certain percentage of fees for the transaction. Some of the well-known acquirers are Paymentech and Wells Fargo. Acquiring institutions sometimes outsource merchant services to third party processing systems like FDC (First Data Corporation), or Global Payment Systems (GPS). Acquiring institutions provide merchants services by using the existing financial network either directly or through third party processing system.

### 3.2 Credit Card Payment Process

A Credit Card Payment is a two step process:

1. Authorization
2. Capture/Settlement

**Authorization**

![Figure 3.2: Authorization with First Data [9]](image-url)

---

10
Authorization is a process in which the merchant verifies the cardholder’s identification and credit limit. The merchant sends the credit card information like the card number, expiration date, and amount to the acquirer. The acquirer will forward the card details to the issuing bank via the existing financial network. The credit card issuer will either return an approval, decline or referral for the authorization request. If the transaction was approved, then the merchant can deliver the goods purchased to the buyer. A transaction can be declined for various reasons like unavailable credit, bad credit history, wrong address, etc. In this case, the seller has the rights to reject service to the buyer. A referral response from the card-issuing bank implies that the response needs more information and normally the acquirer calls the card issuer to resolve the issue.

Capture/Settlement

![Diagram of Capture/Settlement Process with First Data](image)

**Figure 3.3 : Capture/Settlement Process with First Data [9]**

Capture/Settlement is the process of actual transfer of funds from the cardholder’s account to the merchant’s account. As per the regulations imposed for Internet
Commerce, a merchant cannot charge the buyer's credit card until the goods have actually been delivered. Hence the transaction have to happen in two steps. The second step collects the money for the merchant after the goods have been delivered. The merchant initiates a capture in batch mode. The transaction details of the card will be captured and the sale amount will be credited to the merchant's deposit account through the acquiring financial institution and posted to the cardholder's credit card account. There are two types of capture, called terminal capture and host capture. In terminal capture, the authorized transactions are stored in the merchant's software. In the host capture method, the authorized transactions are stored at the acquiring financial institutions or third party processor's host computer.

3.3 Security
In order to retain the faith of existing on-line shoppers and attract new customers, it is vital that the credit card processing software incorporate highest levels of security. The Internet Fraud Watch (IFW) program was established in 1992 by the National Consumers League to monitor consumer fraud. The Federal Trade Commission is attempting to track fraud against business and estimates that fraud, security violations, and theft of intellectual property amounted to $250 million last year [6]. But industry numbers are difficult to track because Internet transactions are not yet differentiated from mail order transactions in credit card processing systems. In an attempt to remedy this, Visa will soon implement electronic commerce flags that track Internet transactions. Internet Fraud is affects both the consumer and the merchant. Internet Credit Card transactions are classified as “Card not present” transactions. Hence merchants are totally liable for the losses even thought the transaction has been successfully authorized before. If the goods do not reach the right consumer, then the merchant will be charged back the amount of transaction. Card Issuing Banks like Visa and MasterCard also charge an amount to the merchant after the charge back limit reaches a specified percent of the merchant’s total transactions. Added to this, there is an additional overhead of fraud detection programs implemented by the merchant to lower the rates. Card Issuers have provided certain tools for detecting fraud in a Card Not Present transaction. Some of these are described below:
Address Verification Service (AVS)

AVS compares the billing address of the credit card number supplied by the merchant with the billing address stored in the card issuing bank’s database. The AVS code returned indicates the level of match that occurred. However AVS works only for US customers. This is an issue especially for merchants who sell on-line because of the International presence of the consumers. The address strings in AVS is not capable of handling non-English multibyte character set that is used by most Asian and European languages. AVS does not protect against fraud when the attacker knows both the credit card number as well as the billing address which is mostly the case with stolen purses or wallets. Merchants using AVS need to pay an additional transaction fees for the address verification service provided for each consumer transaction. This will increase the financial burden on small merchants.

Card Verification Value 2 (CVV2) / Card Identification (CID)

An important new security feature for card-not-present transactions—Card Verification Value 2, or CVV2—now appears on the back of most Visa cards in the signature section after the credit card account number. American Express also has come out with a similar 3 digit called CID. This three-digit number helps validate that the customer is in possession of a genuine and legitimate card. Visa projects a 26 percent reduction in card-not-present charge backs just from the use of CCV2. While this security feature will not be required on all Visa cards until January 2001, approximately 75 percent of all Visa cards already carry the feature, helping merchants minimize fraud, reduce fraud-related charge backs, and improve profitability. Currently the credit card processing application software is being enhanced to include the CVV number.

Secure Electronic Transaction

In 1995, Visa and MasterCard began to develop a standard for processing credit card transactions over the Internet. Called Secure Electronic Transaction (SET), the new standard would not only encrypt transactions but also link them with a digital signature that would fulfill the same role as the physical signature used in stores. Visa and
MasterCard have agreed to treat SET transactions as authenticated transactions so the merchant does not carry the loss and the bank does not assess charge-backs nor chargeback penalties. There are some cons of SET also:

- **Too slow**—Because each SET transactions involves up to 16 transactions, they are compute intensive and slow on today’s computer technology.
- **Too expensive**—While Visa and MasterCard have begun to reduce their transaction fees, banks are still wary that signing up customers for SET will be expensive. Telcos may charge banks as much as $1 per digital certificate, for example.15
- **Too cumbersome**—Banks have yet to figure out how to distribute the software consumers will need to use SET.

Even if the SET adoption rate starts to pick up, without 100 percent consumer adoption, merchants must still have alternative fraud methods as crooks can simply move over to non-SET transactions.

### 3.4 Case Study

Two commercial implementation of credit card processing system are discussed in this paper – First Virtual and CyberCash.

#### 3.4.1 First Virtual

First Virtual was the first Credit Card Processing System started in October 1994 by a company called First Virtual Holding. The product is called Virtual PIN. There is no encryption used. The front-end and back-end software is primitive and used to trade low-value items on the net.

Buyers and sellers had to complete a registration form on the Internet and submit it to First Virtual. Buyer’s registration form had a password to be filled in by the buyer. First Virtual adds a suffix to the password to form a buyer’s Virtual PIN. Virtual PIN would then be sent to the buyer. Buyer, later makes a telephone call to first virtual and provides credit card number. Credit card number is not passed over the network.

Merchants are also given a merchant virtual PIN. On receipt of the PIN, merchants send a check drawn on a bank associated with the merchant to First Virtual through snail mail. First Virtual registers the bank details for the merchant from the check. Merchant is then
set to request First Virtual to process transactions from buyers who have also registered with First Virtual and who make purchases with the merchant.

The following diagram depicts the flow during a transaction using First Virtual:

---

**Figure 3.4: Buying with First Virtual [3]**

---

Buyer chooses an item on the First Virtual Web Server or another Web Server where the merchant is selling. Buyer sends the virtual PIN to the merchant electronically. Merchant forwards PIN to the First Virtual Server. If verification is successful, goods are sent to the buyer. First Virtual Payment Server is notified about the transaction. First Virtual sends
and email to the buyer to confirm whether the goods have been received and are acceptable. If fraud is detected at this point Virtual PIN is blacklisted. If buyer wants to return the goods, payment is not processed. If the buyer accepts the goods or after 90 days since sending the goods, whichever is earlier, the account is billed for the charges. Funds are transferred to the merchant’s account from the buyer’s credit card issuing bank. First Virtual is simple. No encryption is involved. No special software is need at the front or back ends. However there is an overhead in that both the merchant and the buyer need to first register with First Virtual before using it and must have a bank account and credit card respectively. There is no security with First Virtual. Stolen Credit cards can be used to setup virtual PINs. Transmission of virtual PINs across the network is no secure. Attackers tapping the network traffic can intercept virtual PIN numbers and make fraudulent purchases. There could be large amount of virtual Pin usage before fraud is detected since purchases made electronically take only a few seconds. Hence First Virtual is suitable only for either low-value of informative goods.

3.4.2 CyberCash

CyberCash, Inc of Reston, VA was founded in August 1994 to provide software services and solutions for secure financial transactions over the Internet. The CyberCash secure Internet Payment System, which uses a special wallet software, enables consumers to make secure purchases using major credit cards from Cyber cash affiliated merchants. The Cyber cash payment system was launched in 1995 and by mid 1996 over half a million users of Cyber cash were present. The system is mainly used to sell tangible goods.

The figure below describes the payment steps in a CyberCash system.
CyberCash Wallet software is the front-end application of CyberCash that is installed on the buyer's machine that has a web browser. The corresponding merchant software called CyberCash Cash Register is installed on the merchant's machine that has the web server. When the consumer clicks the "Pay" button on the web browser, this message is sent across to the merchant's server. The merchant software sends a summary of the item,
price and transaction id to the consumer's web browser. This message also launches the wallet software on the client. The wallet maintains a list of credit cards owned by the buyer and prompts the buyer to choose from the list. The buyer chooses the credit card that he wishes to use to pay and clicks the wallet's pay button. This initiates CyberCash payment protocol. The card details are securely sent to the merchant. The merchant authorizes the payment with the financial network via CyberCash payment server. If the authorization is successful, goods are delivered to the buyer. The cash register software also does a capture in a batch mode every day. This will result in transfer of funds from the cardholder's account to the merchant through the CyberCash payment server gateway.

As we have seen, CyberCash provides more secure payment method than First Virtual. First Virtual does not make use of a payment protocol. This makes CyberCash more complex than First Virtual. CyberCash has a larger user base than First Virtual. First Virtual is mainly used for low-value and informative goods. CyberCash is used for medium to high value goods since it is less prone to frauds. Both the softwares follow the auth and capture steps. CyberCash is a clear leader in the Credit card processing software.
4. Electronic Check Processing

Checks account for 11% of all the purchases made over the Internet [10]. Electronic Check Processing (ECP) is an electronic payment process designed to debit consumers’ checking accounts for payment of goods and/or services. Corporations can use ECP to centralize, disburse or collect funds from their branches, franchises, agents, or from other corporations. An Electronic Check contains instructions to payer’s bank to make a payment of specified amount to payee. Electronic Check Processing is similar to the traditional check processing in that it adopts the traditional check processing steps to clear checks. However, ECP provides mechanism to verify the funds on-line in real time. The contents of an electronic check are similar to the traditional checks. Signatures on electronic checks are digitized. The ECP procedure is capable of validating digital signatures.

The Financial Services Technology Consortium (FSTC) is an organization involved in introducing a standard for electronic check processing. This organization was founded in 1993 and consists of a group of American Banks.

4.1 Overview

ECP can be achieved in one of two ways for processing:

- by using the **Automated Clearing House (ACH)** network when the customer’s bank is a member of a financial institution, or
- by generating a **facsimile draft**
  - at the direction of the merchant or
  - when the customer’s bank is not a participant of the ACH network

The payer issues a check to the payee. Check contains the digital signature of the payer. The digital signature is generated based on some public key based identity scheme. Variations of an electronic check can provide the functionalities of traveler's check or a certified check. If the currency field is changed, then and electronic check can be used as a traveler's check. If the check contains the signature of the payer's bank, then it becomes a certified check. The consumers are also provided with an electronic checkbook to store
the secret key, certificate information and check information. Digital envelopes are used to transmit the electronic check to the payee. Payee endorses the check using the secure hardware device and forwards the check to the payee's bank. Deposited checks are settled by either directly debiting the customer’s checking account electronically through the ACH system, or by creating a facsimile draft and depositing it on the merchant's behalf (whichever method is deemed better for the transaction). There are 3 steps that occur when the check is forwarded by the merchant's bank to the financial network.

**Validation** occurs on every ECP transaction submitted. The validation process includes format and data edit checks, bank routing number checks and comparison to the data stored in the database.

**Verification** permits merchants to compare each transaction to an external negative file to locate accounts, which have a history of bad checks outstanding or are closed for cause.

**Prenotification** permits merchants to validate account information prior to submitting an ACH transaction for deposit.

If the check fails any of the above checks, then it will be rejected to the consumer. ECP can also handles failures as returns. **The consumer or buyer's bank generates returns (chargebacks).** The bank may return an item for a variety of reasons with no recourse available to the merchant through the banking system. There are, however, certain regulations with which the customer’s bank must comply in order to return an item unpaid. The difference between rejects and return lies in the point of failure. Rejects occur in the financial network and are detected electronically. Returns occur at the buyer's bank for a variety of reasons related to the buyer's account history.

**4.2 Financial Services Markup Language (FSML)**

FSML, the Financial Services Markup Language, is an SGML like mark-up language designed to allow the creation of electronic financial documents. FSML can be used for several applications like creating, and processing Electronic Checks, and their associated documents. FSML does not conform to XML (Extensible Markup Language). The most
obvious difference is that XML requires that every start tag have a balancing end tag, while FSML omits end tags from leaf elements for the sake of brevity.

The Financial Services Markup Language 1.5 is the latest version of the language developed to implement echecks and other secure financial documents. FSML defines a method to structure documents into blocks of tagged content. FSML uses tags to inform processors about how to use the document content in financial applications.

An FSML document contains FSML content blocks. The FSML content blocks in an FSML document can be cryptographically sealed and signed in any combination needed by business applications. Document processors may also remove blocks without invalidating the signatures on the remaining blocks. They may combine signed documents and then sign blocks contained in the combined documents. Signatures and X.509 certificates are structured as FSML blocks. Thus signatures and certificates become part of the FSML document, so they can be verified and counter-signed by later signers.

FSML 1.5 further defines specific block types, content tags, and content for creating payment authorizations, such as echecks. Notably, it defines the tags and content of the block, which contains items such as date, amount, pay to the order of, memo, and so on that would be handwritten on the face of a paper check. It also defines the tags and content of the block, which contains items such as the account number, bank routing and transit number, and other information and restrictions, which would be pre-printed on the face of a paper check. The bank's Certificate Authority cryptographically signs the block, along with the account holder's X.509 certificate, so that no one can alter the block.

4.3 Case Study

4.3.1 Net Check
NetCheck Payment System was developed at the Information Sciences Institute of the University of Southern California. NetCheck is a distributed ECP system that is
implemented using a several connected NetCheck servers. The buyer needs to open a Net Check account with the Net Check authorized bank having the NetCheck server. Electronic Checks are issued using the Net Check bank account. Electronic Checks contain the buyer's digital signature and is also endorsed by the merchant after he receives it. In addition to these, it also contains amount of the check, unit of currency, date, account number, and merchant's name. Net check makes use of Kerberos tickets for creating electronic signatures and endorsing checks. The user first generates the plain text portion of the check. Consumer then contact Kerberos server to generate encrypted digital signature for the check. The check is sent by email over an unsecured network channel to the merchant. The merchant reads the clear text portion of the check and obtains a Kerberos ticket for the consumer's bank from the Kerberos server. The merchant then endorses the check using the encrypted ticket. The check is forwarded to the merchant's bank over a secure link using a Kerberos ticket for the merchant's bank. If the router from the merchant bank to the consumer's bank involves multiple banks in the middle, then each bank appends its signature to the check before sending it forward. Once the check is cleared by the buyer's bank, the signatures are used to trace back the check to the merchant's account. The merchant's account is credited for the amount.

4.3.2 Netbill [Ref 7]

NetBill is an academic project led by Carnegie Mellon University. NetBill transaction is similar to a check in that immediate transfers from the buyer's account to the merchant's account take place. A NetBill server maintains accounts for both consumers and merchants. NetBill servers are linked to conventional financial institutions. A consumer can replenish funds in his NetBill account periodically, using a credit card or bank account; similarly, a merchant can transfer funds from his NetBill account to his bank account as needed.
When a consumer creates a NetBill account, he receives a unique user ID and generates the RSA public key pair associated with that ID. This key pair is certified by NetBill, and is used for signatures and authentication within the system. When the consumer purchases an item on the net, a digitally signed purchase request is sent to the merchant. The merchant computes a checksum, and sends the encrypted goods with a timestamp to the consumer. The front-end software on the buyer's computer calculates a checksum of the goods. Checksum, accepted price, the product identifier, and the timestamp are sent back to the merchant. This information is collectively called the electronic payment order, or EPO.

At this point, the consumer has the goods but cannot decrypt them, and no payment has been made. When the merchant receives the EPO, the merchant's server compares the two checksums and, if they do not match, retransmits the data or aborts the operation. This step ensures that the goods were transmitted without error and to the correct buyer.

Once the goods have been received and verified, the merchant server appends the decryption key to the EPO and then endorses it with the merchant's digital signature. The merchant then sends this to the NetBill server.

The NetBill server verifies that the product identifiers, prices and checksums are all in agreement. If the consumer has the necessary funds or credit in his account, the NetBill
server debits the consumer's account and credits the merchant's account, logs the transaction, and saves a copy of the decryption key. The NetBill server then sends to the merchant a digitally signed message containing an approval, or an error code indicating why the transaction failed. The merchant forwards the NetBill server's reply and (if appropriate) the decryption key to the consumer.

The NetBill server operates **transactionally** to ensure that the consumer does not get billed for goods he cannot decrypt or receive goods without paying for them. The transaction is **atomic**, meaning that all actions occur or none do. If for any reason the transaction can not be completed, NetBill guarantees that the consumer will not be charged.

NetBill uses Kerberos tickets to provide security. The NetBill transaction protocol involves several phases, for price negotiation, goods delivery, and payment; only the last of these phases requires nonrepudiable signatures. Instead of using public key cryptography for message authentication and encryption throughout the NetBill system, symmetric cryptography is used because it offers significant performance advantages.

Recently, Cyber Cash acquired rights to micropayment technology from Net Bill. Cyber Cash will be incorporating Net Bill technology into its range of E-Commerce products.

As observed both Net Check and Net Bill differ from FSTC electronic check processing method. This is because FSTC is a more general-purpose system and not specifically oriented toward check processing. The use of special hardware for FSTC will limit the user base until such time that the special hardware is cheap. Both Net Check and Net Bill are academic research projects that have gained acceptance in the industry. They are specifically targeted towards check processing and not meant to cover other payment methods.
5. Electronic Cash Payment System

Cash Payment is the earliest and the most popular form of payment. About 80% of the total payment in the world is through cash [3]. Hence it is vital to improvise cash payments electronically. Cash is attractive mainly because of guaranteed payment to the merchants, without overhead of transaction charges. Criminals are also fond of cash because cash payment does not leave audit trails.

David Chaum who is called the "father of digital cash" first proposed the concept of electronic cash. Electronic cash offers added convenience and costs involved for banks and merchants are greatly reduced. Consumers need no longer fiddle for exact change in certain circumstances or burdened down by carrying coins or cash.

5.1 Overview

Electronic Cash Payment System attempts to imitate the conventional cash payment. They attempt to maintain anonymity and at the same time provide security. There are two ways in which Electronic Cash Payment Systems can be implemented: using Smart Card Technology or using an electronic mint. Each of these technologies is discussed using an example in the case study section.

5.2 Case Study

5.2.1 Ecash

DigiCash, a company that was founded by David Chaum, developed Ecash. Ecash provides both security and anonymity needed for cash payments. Entities in an Ecash system are merchant, consumer and Ecash bank (also called as Mint). Consumers and merchants open an account with the Ecash Bank.

Ecash provides front-end software called Ecash cyber-wallet that resides on the consumer's computer. CyberWallet stores and manages consumer's coins, and keeps record of all transactions. Consumer first withdraws coins from Ecash bank to their wallet.
software on the local disk. The withdrawal protocol prevents a bank from being able to see the serial numbers of the coins it is issuing. This is done to provide anonymity.

Ecash coins are minted by the consumer and signed by the bank. Each coin has a serial number that is generated by the customer's wallet software using random number generation schemes. The serial number is masked and sent to the bank so that the bank cannot log the serial numbers of the coins with a particular customer. The customer also request that a certain value be assigned to the coins. The bank checks the consumer's account to determine whether the consumer has the amount desired to be stamped on the coins. If the consumer has the desired amount, the bank signs the coin blindfolded and assigns a denomination to it. Consumer's account is deducted by the denomination. Coins are sent back to the wallet. Walled decrypts the coins and makes it ready for use.

When the customer chooses to purchase an item on the web, the customer sends the request to the merchant. The merchant responds by sending a payment request to the client. The payment request contains the currency to be used, amount, timestamp, merchant bank ID, merchant account ID and a short description. This request is not encrypted which makes it unsecured. If the consumer decides to pay, coins valuing the requested amount are gathered from the wallet and the exact amount is sent to the merchant. The wallet is capable of withdrawing new coins from the Ecash Bank if more denomination is needed to make a payment. The merchant forwards the coins to the Ecash Bank. The Mint verifies that the consumer has not already spent the coins. If the consumer has not yet spent the coins, the coins will be deposited in the merchant's account. The merchant then sends the goods and a receipt to the customer. Refunds and payout services are also handled in the same way but this time payment is originating at the merchant and ending at the customer. Ecash Bank is not capable of processing coins from other banks. Similarly Ecash coins cannot be processed at other bank. This is a severe limitation in propagating electronic cash payment. However, as this method becomes more and more popular, third party banks could come up that will process coins from multiple banks.
5.2.2 Mondex

Mondex is a cash payment scheme that was initially funded by a major banking organization called National Westminster (NatWest) in U.K. In June 1996, Mondex International became a separate company to promote the technology around the world.

Mondex payment system involves the use of an electronic card called Mondex card that is loaded with money from an account. Mondex card is an integrated circuit card (ICC). It is a form of smart card containing a small microcomputer chip embedded on it. The chip is programmed to function as an "electronic purse". The electronic purse is the front-end software for the Mondex system. The purse is capable of handling five different currencies at a given time. It can store a record of the last ten transactions. The card is secured through a code chosen by the consumer. Mondex electronic cash can be transferred from consumer to merchant, or to conduct transactions between consumers without interaction from external banks.

There are six entities involved in a Mondex Architecture. Franchisees are entities who are granted the right and obligations to manage and promote and exploit Mondex in their geographic territory. Originators issue, control and redeem electronic cash denominated in a currency. Members are licensed by Franchisees to issue Mondex cards to consumers and merchants in the Franchisee's territory. They obtain Mondex cash from the Originator and sell it to consumers and merchants. They also purchase excess balances from consumers and merchants. Manufacturers produce the hardware need to process Mondex Cards and sell it to Mondex users. Merchants enter into an agreement with Members to enable them to accept Mondex electronic cash as payment for goods or services. Cardholders are consumers who are provided with a Mondex card by the Members and pay for goods or services received from the merchant.

The consumer initially registers with the Member. Member provides the consumer with a Mondex Card. Consumer can load it with cash from a bank using Mondex ATM. At the bank side, a hardware device called Mondex Value Box is installed. This device is like a
money safe that can hold large number of Mondex cards and also talk to a Mondex ATM to load money on to the card. Mondex Value Box is maintained by software called Value Control and Management System. This software controls transfer of money to and from the value box to the cards and maintains the record of those transactions. Merchants have hardware known as value transfer terminal. When a consumer presents Mondex card to the merchant, the Value transfer terminal transfers the amount from the consumer’s card to the merchant's card. There is no online transfer to the bank for the transaction to be completed. As a batch process, the merchant contacts the bank at a later stage to actually transfer funds to the merchant's account.

Security is provided at two levels in Mondex. The chip used on Mondex cards has in-built risk management system. This system will close down the card under unusual card behavior like transfer of huge funds etc. When cards are issued, each contain two different and separate security schemes, A and B - each comprising one or more 'keys' or more cryptographic algorithms or other security features. Initially cards will be set to operate on scheme A but consumer can change the security scheme to alternate B one. Merchants can lock the Value Transfer Terminal with a PIN code so that only authorized personnel can remove value from the Mondex merchant's terminal, or allow refunds.

Electronic Cash Systems have need a lot of backing from the banking industry. Because these systems try to maintain anonymity of the transactions, financial institutions are hesitant to implement this. In this market, technology is successful if big movers back it. Cash Payment Systems involve considerable amount of hardware equipment. It is important that the costs of the required hardware be considerably reduced so that general public can use the cash payment system.
6. Analysis and Comparison of Payment Methods

6.1 Architecture

Credit Card Processing System makes heavy use of the underlying banking infrastructure to authorize and settle payment. The banking infrastructure is built on a legacy system that was initially optimized for older systems. In the present world, although there have been major improvements in terms of upgrading the banking infrastructure, a significant amount of work needs to be done to make the banking infrastructure more efficient and faster. Electronic Credit Card Processing is like having a front-end with the latest technology for a back-end that was not originally designed for it.

Credit Card Systems are designed to handle complex payment needs like refunds, charges and returns. The protocol followed for each of these cases is different from the payment protocol. Credit Card Transactions always happen in two steps - authorize and capture. Credit Cards can be used for making either low or high value payments.

Electronic Cash Payment Systems do not need to contact the bank at the time of processing the payments. The underlying architecture for the back-ends was designed specifically for making electronic payments unlike the credit card back end architecture. Hence cash payment systems are have a better overall architecture and are not just hacked to work. Electronic Cash Payment Systems are totally different from the existing network.

Electronic cash systems do not have explicit methods for refunds, charges or debits. The same protocol is adopted in the reverse direction, originating from the merchant and ending at the customer. Electronic Cash Payment System completes transactions atomically in one step. Electronic Cash Payments are normally used for making low value payments. They are unsuitable for high value payment because they are less secure and preserve anonymity of transactions.
Electronic Check Payment System proposed by FSTC also makes use of the Automated Clearing House to process electronic checks. This is similar to the existing Credit Card architecture. But unlike Credit Card no on-line authorization is required by electronic checks. Checks are batched and set to the clearinghouse periodically.

Electronic Checks are designed to handle returns from the payee's bank. They however do not have the concept of refund. Checks are processes sequentially from the payer to the payee's bank in one step involving anywhere from a few hours to a day. Electronic Checks are used to make low to medium value payments.

6.2 Security

Credit Card Payment Methods adopts SET protocol as the standard for secure payment transactions. Electronic Check and Electronic Cash payment methods do not have a standard protocol for securing the transactions. Hence most of the times standard protocols like Kerberos, RSA or SHA are used for Electronic Check and Electronic Cash Payment types. It is important to develop a standard protocol for check and cash payment types. Protocols meant for a specific application makes it more secure. Credit Cards also have AVS and CVV2 for verification and authorization. This adds security to credit card processing. Electronic Checks digitize signatures and transmit checks within a digital envelope. Electronic Cash systems have electronic cash banks (Cash servers) that digitally sign the coins to be issued to a customer.

6.3 Cost

Credit Card Transactions involve an overhead in terms of on-line authorization and batch settlement needed from acquiring institutions. The rates vary among different acquiring institutions. However if the merchant has lower number of transactions with a small value amount, then the overhead incurred will be higher in terms of the percentage.
From the graph above, the cost per transaction is lowest in the US, followed by Europe, Latin America and Asia. Over the past 5 years, costs have dropped by 400% in the US from 4 cents to 1 cent per transaction. Competition and the need to lower prices to customers drive these decreases. Higher costs mean less number of small business merchants opting for credit card processing and hence lesser consumers utilizing this facility. This beats the objective of electronic payment types.

Electronic Cash payment types have one-time installation expense. Smart Cards require a special chip to be present on the card. Their needs to be hardware card readers, hardware balance readers for the card, and also on the merchant side hardware smart card processing equipment. Hence these payment types have lower on-going expenses. But, they do have a higher installation expense since some special hardware is needed to process them.

Electronic Checks have the lowest cost. The transaction fees charged by ACH to process electronic checks is lower than that of credit cards. The process of digitally signing a check and masking it inside a digital envelope involves purchase of special software to do that. But it is a one-time expense and is not incurred with time unlike credit cards. It has also been reported that the number of fraudulent transactions is lower with electronic checks resulting in lower expenses.
6.4 Scalability

The slide shows increasing transaction volumes for Credit Card processing in European markets. The first bar represents the 1996 card volumes and the second set of bar represent the 2002 card volumes. It is expected that by 2000, acquirer FDC is expected to see 30mm transactions per day. Under these conditions, it becomes imperative for acquirers to be able to expand their existing architecture to expect exploding growth. The current architecture for Credit Cards has been demonstrated to be scalable. However, the scalability still remains a question for Electronic Check and Electronic Cash payment systems.

6.5 Flexibility

Flexibility is needed in any payment system to handle new protocols, to change terms on existing products, to change offers to specific customer segments, and finally to change the workflow pattern across all aspects of data center.

Credit Card Systems have demonstrated ability to accommodate new types of cards and to handle ever-changing protocols. The SET protocol used by Credit Card Processing is very open-ended making it more flexible. However the electronic cash systems (like Mondex and Ecash) are based on proprietary protocols and proprietary architectures. This makes it difficult to adapt these products for any changes. Another major drawback of
being proprietary is that of integrating these products with other applications like Billing Software. Ecash system is not able to process coins from other banks. Similarly other banks are not capable of processing Ecash coins. Hence there is no open-end architecture for Ecash payment systems. Electronic Check Payment Systems are being standardized by FSTC. FSTC's check payment processing is yet to be incorporated into commercial products and accepted as a standard.

6.6 Performance

Credit Card Processing System requires on-line authorizations. This means delays resulting from slow transmissions across the network. As the graph indicates the number of credit card transactions are consistently increasing. So, it is important that we work towards eliminating the delays associated with on-line authorizations needed for each transaction. Electronic Cash and Electronic Check have all the necessary data available on the hosting server. Hence these systems need not contact financial institutions on-line.

6.7 User Base

![Technology Trends: More Monetary Instruments](image)

In the earlier days, commodity money, conventional cash were most popular because they were the only payment types available. However with time, banks came into existence and the society underwent a financial revolution. In the 1900, we are seeing multiple
payment methods. Since most of these methods are new, there are no clear-cut trends as to which payment type will establish itself.

Conventional cash payment type accounts for nearly 80% of payments made in the world. Among the non-conventional-cash payment methods available, Credit Cards are the most popular in the US while Electronic Cash in the form of Smart Cards are popular in European countries. It is estimated that there will be 2 billion smart cards in use by 2000 accounting for 25% of US's payment method. The popularity of credit cards is mainly because of the usage of known banking institutions. People are more confident of dealing with large bank names instead of trying to jump into a new software for Electronic Cash and Electronic Check. However with time, more and more people will slowly get used to using software for Electronic cash and check.
6.8 Ease of Use

Credit Card payment can be done without the need of sophisticated software at the consumer site. Credit card numbers can also be just told over the phone to make a payment happen. Most of the people in the US have the basic know-how of using a credit card. Minimal or no training is needed for customers to make payments using credit cards.

Electronic Check payment system needs installation of software and sometimes special hardware at the customer site to be able to create and process electronic checks. Electronic checkbooks are also maintained at the customer site. People need to be trained to use the special technology for issuing electronic checks.

Electronic cash payment system has a special software called electronic purse that needs to be installed at the customer site. The purse will store coins, maintain the balance and communicate with the electronic cash banks. People need to be trained to use electronic purse.
7. Future of Electronic Payment System

There are a wide variety of payment systems available to a consumer today. However there arises a need to provide a single universal payment system that provides the advantages of all the existing payment system. In an effort towards this direction, an organization called Joint Electronic Payment Initiative (JEPI) has been formed. The objective of this group is to define a set of protocols and interfaces that can support the use of a wide variety of payment methods for network commerce.

It is clear that Credit Card Payments have adopted SET as a standard for payment transactions. However, no protocol is currently available for electronic check payment. Financial Service Technology Consortium (FSTC) is working towards bringing in a standard for electronic checks. FSML has been introduced to develop secure financial documents like checks. However, it is yet to be accepted as an industry wide standard. Electronic Cash products like Ecash that do not make use of banking infrastructure are finding it difficult to push into the market. However smart card systems like Mondex are not popular in the market because of not being backed up by major banking institutions. We should try to develop systems that are not proprietary and inflexible but instead are open-ended.

Electronic Payment Industry has an extensive potential for growth considering the growth of Internet. We should take advantage of this and make the best use of available technology for the betterment of mankind.
References

1. Making Money in cyberspace by Paul and Sarah Edwards, Linda Rohrbough
2. Smart Cards by Henry Dreifus, J.Thomas Monk
3. Electronic Payment Systems by Donal O'Mahony, Michael Peirce, Hitesh Tiwari
4. Smart Cards, The Global Information Passport by Jack M. Kaplan
11. http://www.telecheck.com