Changing Money: Cash and Cards, Virtual and Electronic

Setsuko Minamikawa

March 1998

Program on Information Resources Policy

Harvard University

Center for Information Policy Research

Cambridge, Massachusetts

A research draft of the Program on Information Resources Policy.

Changing Money: Cash and Cards, Virtual and Electronic

Setsuko Minamikawa
March 1998

Project Director
Anthony G. Oettinger

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

March 1998

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

AT&T Corp.
Australian Telecommunications Users Group
Bell Atlantic
Bell Canada
BellSouth Corp.
The Boeing Company
Cable & Wireless (U.K.)
Carvajal S.A. (Colombia)
Center for Excellence in Education
Centro Studi San Salvador, Telecom Italia (Italy)
CIRCIT (Australia)
Commission of the European Communities
Computer & Communications Industry Assoc.
CSC Index (U.K.)
CyberMedia Group
DACOM (Korea)
Deloitte & Touche Consulting Group
Dialog Corp.
ETRI (Korea)
European Parliament
FaxNet Corp.
First Data Corp.
France Telecom
Fujitsu Research Institute (Japan)
GNB Technologies
Grupo Clarin (Argentina)
GTE Corp.
Hearst Newspapers
Hitachi Research Institute (Japan)
IBM Corp.
Intel Corporation
Investment Company Institute
Korea Telecom
Lee Enterprises, Inc.
Lexis-Nexis
Lincoln Laboratory, MIT
Litton Industries, Inc.
Lucent Technologies
John and Mary R. Markle Foundation
Microsoft Corp.
MicroUnity Systems Engineering, Inc.
MITRE Corp.
National Telephone Cooperative Assoc.
NEC Corp. (Japan)
The New York Times Co.
Nippon Telegraph & Telephone Corp. (Japan)
NMC/Northwestern University
Pacific Bell
Pacific Bell Directory
Pacific Telesis Group
The Post Office (U.K.)
Raytheon Company
Research Institute of Telecommunications and Economics (Japan)
Revista Nacional de Telematica (Brazil)
Samara Associates
Scaife Family Charitable Trusts
Siemens Corp.
SK Telecom Co. Ltd. (Korea)
Strategy Assistance Services
TRW, Inc.
UNIEMP (Brazil)
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - Defense Intelligence Agency
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of the Treasury
  - Office of the Comptroller of the Currency
- Federal Communications Commission
- National Security Agency

United States Postal Service
Viacom Broadcasting
VideoSoft Solutions, Inc.
Weyerhaeuser

Note

This report offers an overview of the electronic payments systems arena as of early 1997. The issues discussed concern current major electronic payments system providers: who they are and what kinds of services they provide, as well as such issues as security, privacy, legal and regulation, which are prominent in this field.

Because developments in the electronic payments system change so rapidly, it is barely possible to gather every bit of information in this field. This paper has therefore concentrated on developments in the United States market. The United States is one of the most advanced countries in electronic payments systems, owing to extensive deployment of both information infrastructure and financial networks. To avoid predictions of what may not, after all, occur, the report does not offer prospective comments or evaluations, but, instead, provides only facts as of early 1997.

Contents

Illustrations

Figures

Tables

Chapter One

What Is Money?

Although the new electronic payments systems are being talked about in newspapers, magazines, and on the Internet and people say that how everyday payments are conducted will change in the near future, as of the mid-1990s most retail financial transactions remain paper-based. According to a 1995 telephone survey commissioned by the United States Federal Reserve cash transactions accounted for 18 percent of the expenditures of the average adult in the United States, compared with roughly two-thirds for checks and 13 percent for credit and debit cards.[1] Because payments for credit cards are usually paid by check, the use of checks is not disappearing. In 1994, the total volume of check transactions in the United States was 62 billion—32 percent more than in 1985 (see **Figure 1-1**). Several years from now, the system will most likely still be largely paper-based. According to one estimate, roughly 80 percent of consumer payments will still be in the form of cash or check by the year 2000 in the United States.[2]

Some changes, however, have taken place, as indicated by the increasing number of automatic teller machines (ATMs) and point-of sale (POS) terminals, which offer customers alternatives for meeting payment needs. ATMs, along with bank branches (**Figure 1-2**), are increasingly common in shopping malls, and the number of POS terminals has expanded rapidly (**Figure 1-3**). A notable new way to make payments is by use of POS terminals, which require debit cards. A debit transaction is a direct substitution for a check (and, in some cases, for cash) and may represent the beginning of a transition from paper-based systems to electronic payments.[3]

Understanding the issues involved in the use of electronic money requires understanding the nature of money. Money typically has three basic functions:

1. It is a unit of account, that is, a way to measure and record value: e.g., a pig is worth X dollars.

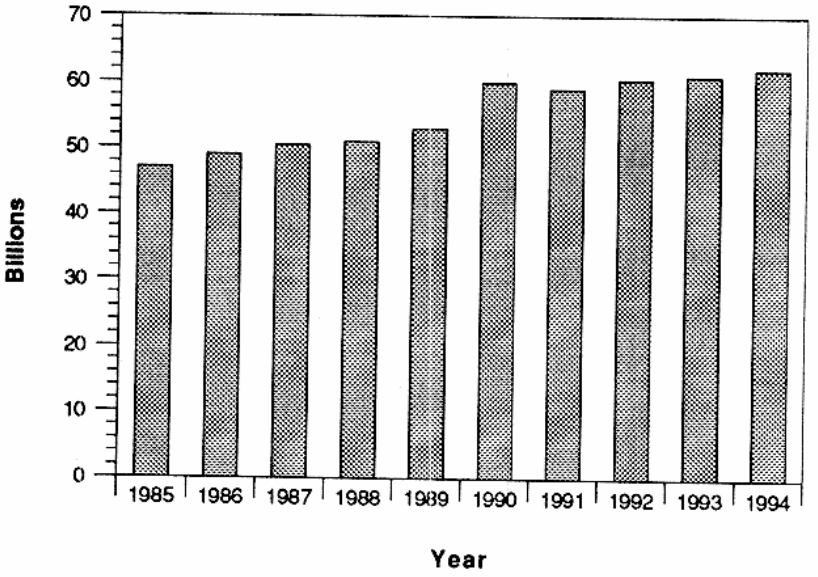
2. It is a store of value, that is, a convenient way to store value for future use: possession of a pig is replaced by possession of a bank account.

---

[1]United States Congressional Budget Office, *Emerging Electronic Methods for Making Retail Payments* (Washington, D.C.: U.S. Gov't Printing Office, June 1996), 17.

[2]American Bankers Association, *The Role of Banks in the Payments System of the Future,* September 1996, 7-8

[3]Ibid., 9



Source: American Bankers Association, *The Role of Banks in the Payments System of the Future*, 1996.

Figure 1-1

Volume of Check Transactions in the United States in 1994

3. It is a medium of exchange: instead of first needing to find a pig to trade for cloth, money buys cloth or a pig.[4]

As a medium of exchange, according to Marvin Sirbu, of the Information Network Institute at Carnegie-Mellon University, "money has progressed from being itself valuable (cows, eggs); to currency convertible to something considered valuable (gold), which requires faith; to the blind faith that the piece of paper will be accepted."[5]

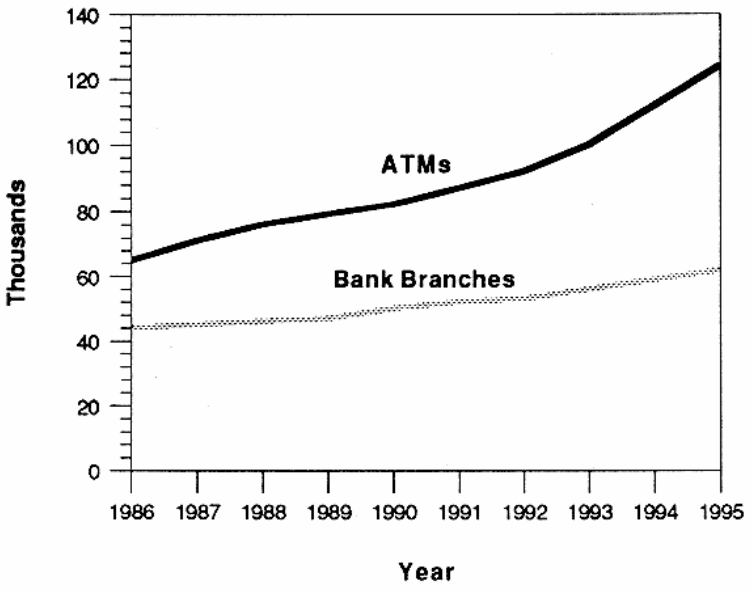
According to Mitsuo Yamaguchi, of the Hitachi Research Institute, six features characterize the convenience of cash:

- Acceptability (cash can be used anywhere)

---

[4]Edward W. Kelley, Jr., "The Future of Electronic Money: A Regulator's Perspective," *IEEE Spectrum* **34**, 2 (1997), 21-22.

[5]David Bollier, *The Future of Electronic Commerce*, A report of the 4th Annual Aspen Institute Roundtable on Information Technology, Aspen, Colorado, August 17-20, 1995 (Washington, D.C.: The Aspen Institute, 1996), 25.



Source: American Bankers Association, *The Role of Banks in the Payments System of the Future*, 1996.

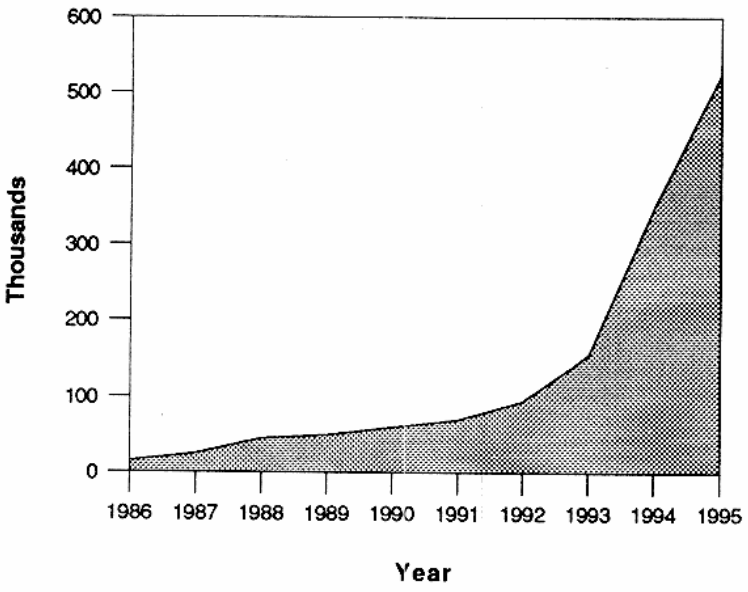
Figure 1-2

Number of ATMs and Bank Branches

- Continuity or transferability (credit cards are closed-loop payment, whereas cash can be used to pay for another customer's change)
- General-purpose (can be used to buy anything)
- Finality (settlement is finished at the time of payment; no authorization is needed)
- Security (forging notes is generally difficult), and
- Anonymity (cash cannot be traced—who bought what—thus, it protects privacy).

Cash, however, has its own weaknesses:

- Payment can only be made in person. Remote payment cannot be made, because sending cash by ordinary mail is prohibited.
- Cash is not divisible: a $10 bill cannot be physically divided into $4 and $6 (a $10 note must be changed into smaller notes).



Source: American Bankers Association, *The Role of Banks in the Payments System of the Future*, 1996.

Figure 1-3

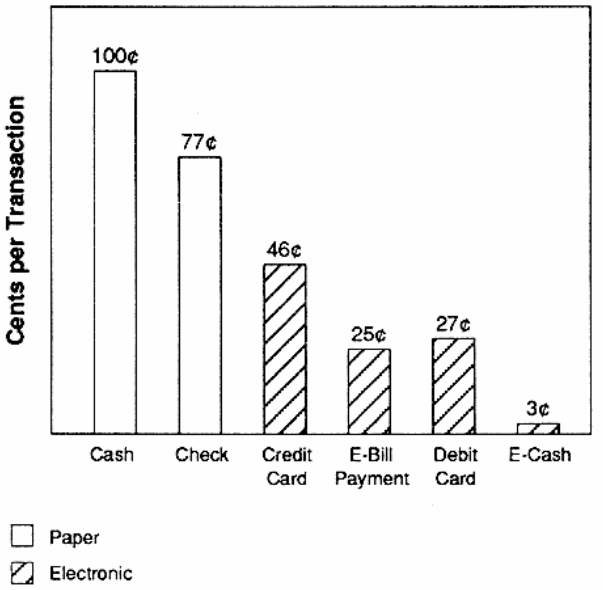
Point-of-Sale (POS) Debit Terminals

- Handling cash is expensive. According to David B. Humphrey, of Florida State University, it is approximately 2.8 percent of the gross domestic product (GDP).

- From the viewpoint of protecting the natural environment, it is difficult to ignore the amount of pulp consumed and processing of ink.

Electronic cash has the potential to become a superior medium of exchange. In comparison with traditional cash, it can be transferred at great speed over great distances, is more secure than cash or checks, and can create instant settlement transactions. Electronic cash may help simplify the complex network of modern commerce. Its lower processing costs make it very attractive to businesses (**Figure 1-4**).

The question it raises is, can people trust that their electronic cash will be accepted and will electronic cash be backed up by guaranteed value? The success of electronic cash may largely depend on whether it serves the functions of traditional money better than the existing forms do. Its acceptability will be determined by the market. Consumers will want to have products that are convenient, easy to use, priced at what they are willing to pay, with plenty of locations at which electronic cash can be used. Solid security measures also will be important and necessary to reduce apprehension.



Source: American Bankers Association, *The Role of Banks in the Payments System of the Future*, 1996. Based on data from The Boston Consulting Group and the Federal Reserve Board.

Figure 1-4

Electronic Money and Paper Money: Comparison of Cost per Payments Transaction

Chapter Two

Major Categories of Electronic Payments Systems

The developments in electronic payments systems are occurring so quickly that, rather than attempt to offer a paradoxically complete view of flux, the objective here is to provide a reasonably representative sampling.

Electronic payments systems can be divided into two major groups (see **Figure 2-1**):

1. Payments on the Internet
   - DigiCash's "ecash"
   - Cybercash's "CyberCoin"
   - CheckFree's "CheckFree Payments Services"
   - Financial Services Technology Consortium's "Electronic Check"
   - Security First Network Bank's "Security First Network Bank"
   - First Virtual Holdings' "Internet Payment System"
2. Payments by Stored Value Cards
   - National Westminster Bank's "Mondex"
   - Visa International's "Visa Cash"

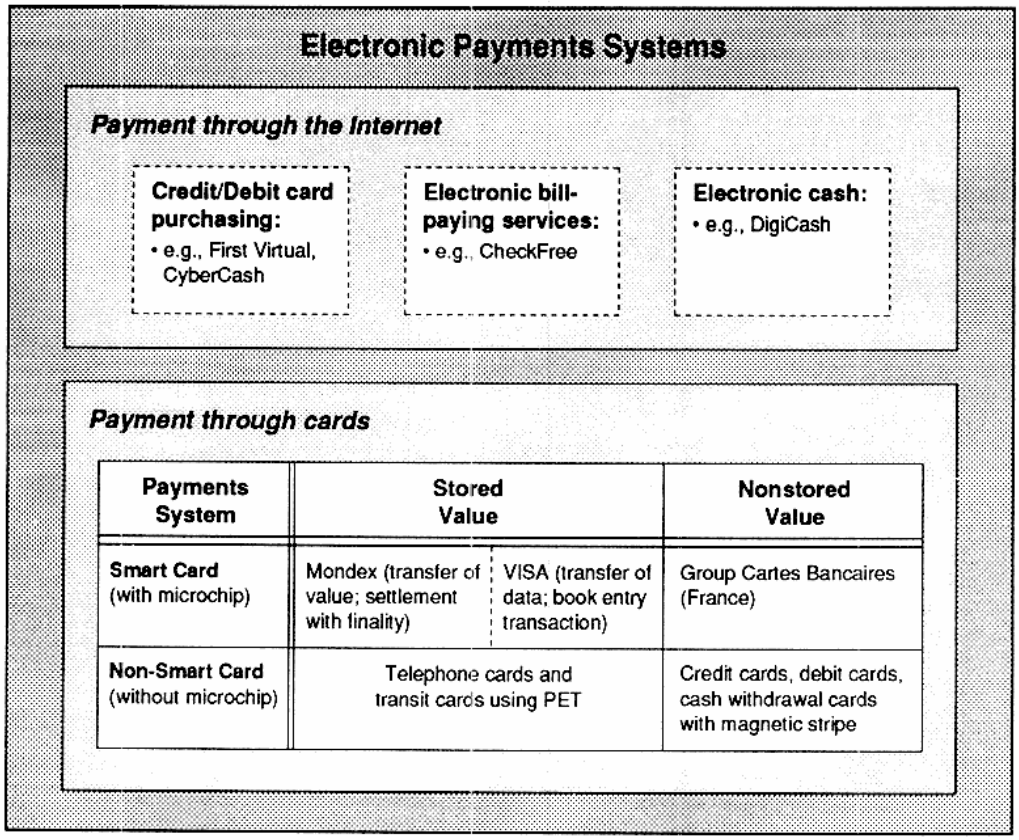
Many services, described in this report as of March 1997, are in experimental stages. Many are evolving for greater convenience, variety, and security and will probably be changed further and upgraded. Companies are keen on collaborating, in order to provide wider services as well as to standardize technology, and partnering with other companies for technology development.

2.1 Payment on the Internet

Present electronic payments services provided for Internet purchases according to the terms listed above can be further subdivided into three groups: credit card purchases, electronic bill payments, and electronic cash (see **Figure 2-1**).

2.2.1 Credit Card Purchases

First Virtual Holdings. First Virtual Holdings claims to be unique in its security in using traditional technology already in the market. Its security is maintained by letting the customer register the credit card number at the start of service. In a sense, First Virtual is not offering true electronic cash (see section **2.1.3**) but an intermediary form of convenient electronic payment.



PET = Polyethylene Terephthalate

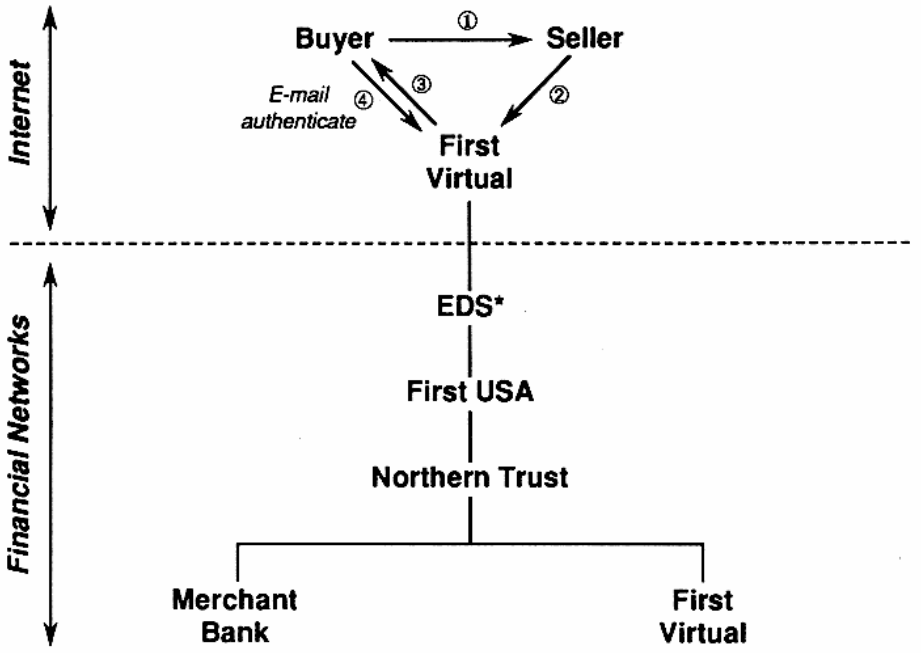
Source: Hitachi Research Institute.

Figure 2-1

Categories of Major Electronic Payments Systems

To use First Virtual's service, a customer must have an electronic mail (e-mail) address; a Virtual personal identification number (PIN), provided when one becomes a member; and a credit card (the number is registered at the start of service). To use the service, a merchant must have an e-mail address; a Virtual PIN; and a checking account, to receive payments. See **Figure 2-2**.

CyberCash. CyberCash, based in Reston, Virginia, is aggressively expanding its presence in the electronic payments market by working jointly with financial institutions such as NationsBank Corp., First Union Corp., First U.S.A, Inc. and PNC Bank Corp. CyberCash has technology partnerships with such companies as CheckFree, Verisign, and RSA Data Security.



① Buyer gives seller a purchase order with ID number.
② Seller transfers purchase order to First Virtual.
③ First Virtual confirms purchase order.
④ Buyer acknowledges purchase order.

*EDS provides data processing, identification numbers, credit card numbers, and e-mail addresses.

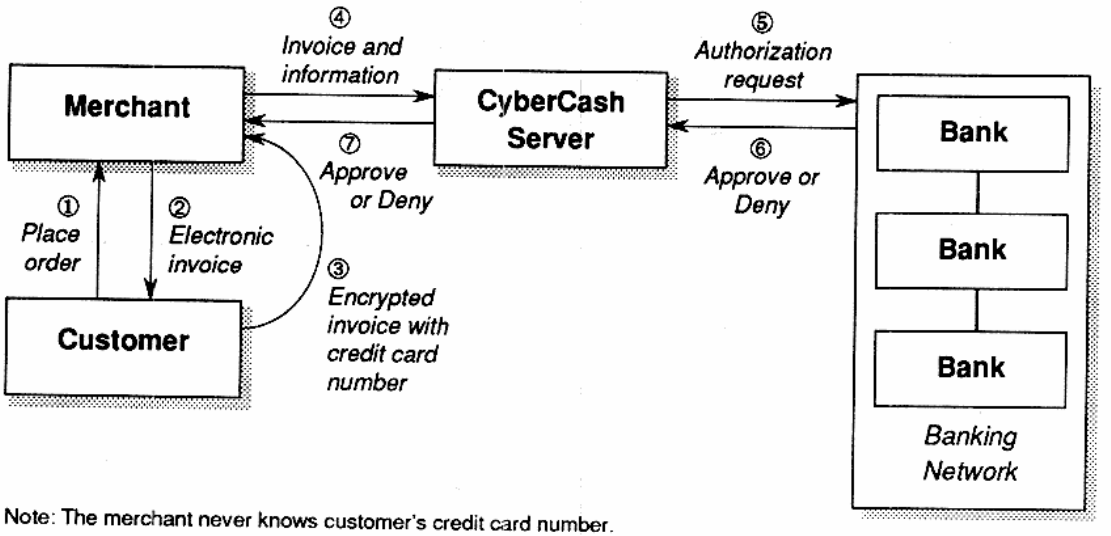
Source: Adapted from a conference slide of First Virtual Holdings.

Figure 2-2

First Virtual's Service Flow

CyberCash offers two categories of service, credit card purchases and CyberCoin. It calls the combined service "CyberCash Wallet," to indicate that, as in everyday life, an individual may select a method of payment.

In early 1995, CyberCash started its credit card purchases service (see **Figure 2-3**). In a way, CyberCash credit card purchases are not a totally new type of payment—the service does not transfer monetary value to the consumer. Instead, it allows the customer to transmit a credit card number over the World Wide Web (WWW) with secure encryption. When the customer decides to make a credit card purchase using CyberCash, the merchant sends the customer an electronic invoice over the WWW. The customer reviews the invoice and, if it is correct, appends the credit card number to it. Then, CyberCash software encrypts the credit card portion of the invoice and returns it to the merchant. The merchant appends its own confirmation number, encrypts the entire package, and forwards it to a CyberCash server for reformatting and encryption in banking formats. The CyberCash server then sends the



Note: The merchant never knows customer's credit card number.

Figure 2-3

CyberCash's Credit Card Transaction

package to the banking network, where it is treated as an ordinary credit card transaction.[1] Messaging and security both are software-based.

CyberCoin service allows Internet users to buy low-price online goods and services from participating merchants. CyberCoin is suitable for purchasing goods on the Internet, and a new type of merchant is already emerging, such as offering small pieces of digitized information, for a price as low as 25 cents. By offering a low transaction fee to merchants, the new CyberCoin system smoothes the path to conducting small transactions on the Internet. Currently, credit card transaction fees make it unprofitable for merchants to sell goods or services for less than $10.

Introduced in September 1996, CyberCoin was designed to support small (25 cents to $10) transactions for information goods over the Web. The customer opens a virtual account called a CyberCash account and receives CyberCoin through the bank account. Thus, CyberCoin is charged as prepayment data to CyberCash Wallet. When the customer makes a purchase on the Internet, the customer transmits CyberCoin to the merchant, and CyberCoin is transmitted to the merchant's CyberCash account.

---

[1]Daniel C. Lynch and Leslie Lindquist, *Digital Money: The New Era of Internet Commerce* (N.Y.: John Wiley & Sons, Inc., 1996), 27.

Actual settlement is implemented by fund transfer from the customer's bank account to the merchant's bank account through the existing bank network automated clearinghouses (ACHs) after the transfer of CyberCoin is completed. The settlement between the merchant and customer is batch processed, for efficiency.

Through this CyberCoin service, known as a micropayment system, merchants that, owing to a lack of any feasible payments system, often had to give away information (such as micropublishing [newspaper articles], pay-to-view or pay-to-play transactions, or online gaming or online chat, or software distribution, music, etc.) now can be compensated for their efforts. CyberCash charges merchants between 8 to 31 cents for transaction amounts ranging from 25 cents to $10.

2.1.2 Electronic Bill Payments

CheckFree. CheckFree, established in 1981, is a major bill payments service based in Columbus, Ohio. CheckFree Payments Services were started in 1995, as a bill payments processing service on the Internet. Its customers are mainly individuals and merchants; an individual signs up with CheckFree to pay bills electronically, and a merchant signs up to receive payments electronically.

CheckFree provides an electronic bill presentment and check payments service called "E-Bill." With E-Bill, the user can receive bills and pay them on-line via the Internet, and to confirm sent information, such as payee and amount, the user clicks the "transmit" button—and payment is done. CheckFree also provides a payments service using the telephone: calling a toll-free number, the user can say whom to pay, when, and in what amount. The user can schedule payments by using either touchtone buttons or spoken commands. For payments to smaller merchants or to individuals, CheckFree may send a laser-printed check through the U.S. Postal Service. Payments are recorded on the subscriber's monthly bank statement or included in canceled checks, depending on how the checks are processed. For CheckFree subscribers using PCs, the software (provided by CheckFree) keeps a record of their transactions. Telephone service subscribers receive a monthly statement of transactions from CheckFree or from the financial institution offering the CheckFree service. CheckFree offers security mainly because (so far) it relies on traditional means of electronic funds transfer (EFT) through telephone and modem, rather than on the Internet.[2]

The Financial Services Technology Consortium (FSTC). The FSTC was founded in 1993 to develop payments systems for electronic commerce. Sixty U.S. organizations

---

[2]Ibid., 24-26.

participate, including financial institutions, clearinghouses, universities, and companies. Among well-known banks, participants include Bank of America, Citibank, and Chemical Bank.

In September 1995, the FSTC began testing an electronic check system on the Internet called "Electronic Check," one of five major development projects of the FSTC. The others include check truncation,[3] electronic commerce, security measures, and a smart card system. In the electronic check system, a consumer with an electronic checkbook on a Personal Computer Memory Card International Association (PCMCIA) card writes a check electronically from the checkbook on the card and then sends it to the retailer over the Internet. The retailer sends the electronic check to the customer's bank over the Internet, and settlement is made through a financial network, such as an ACH. In addition to payment data, commercial data, such as invoice number and date of deposit, can be shown on the electronic check; the efficiency achieved by conveying invoice and remittance information allow payments to be linked into accounts payable and accounts receivable processing systems. To make the system more practical, the FSTC plans to adopt a smart card as an electronic checkbook, but so far this concept remains in an experimental stage and may take time to enter practical use.

Security First Network Bank (SFNB). SFNB, originally a subsidiary of Cardinal Bancshares but now an independent organization, opened business on the Internet in October 1995. As of early 1997, access to its products was limited to U.S. citizens. SFNB's business is conducted on the Internet and by telephone and mail. It competes in convenience (any time, anywhere with a PC) and price (very aggressive). Its lower cost structure allows lower pricing, compared with traditional banking with tellers.[4]

SFNB is different from other electronic cash issuers, such as DigiCash; it is a virtual bank, and its main business is providing banking services over the Internet. A customer can open an account at SFNB, either a checking account or both checking and savings. To open a checking account, a customer sends a deposit by check or credit card (minimum of $100) through ordinary mail. Management fees depend on the balance, just as with any neighborhood bank. The idea of SFNB's services is for a customer to manage accounts and bills on the Internet. A customer can pay bills through SFNB electronically, using electronic checks, and transfer funds electronically.

---

[3]Truncation is sending electronic data for remittance, instead of transporting checks physically.

[4]Andersen Consulting, *Financial Services in a Virtual World* (London: 1996).

2.1.3 Electronic Cash

The term "electronic cash" implies that monetary value that is electronic exists *with* the customer. By contrast, credit card purchases on the Internet (as in First Virtual's system) involve customers giving payment instructions to move money from the customer's bank account to the merchant's bank account. The main difference between electronic cash and credit card purchases is where the money is located]. For example, with electronic cash (such as DigiCash's "ecash" and Mondex, section **2.2.1**), when a customer downloads money, say, $20, from a bank account, that $20 is transferred to the hard disk of the customer's PC (DigiCash) or to a card with an integrated circuit (IC) chip (Mondex), both directly within the customer's possession. (Dan Eldridge, DigiCash's vice-president for business development, likened "ecash" to travelers checks, because it is a *bearer's instrument*.)[5] With credit card purchasing services such as CyberCash and First Virtual, the money remains in the bank, moving only from the customer's account to the merchant's account. In this report, the term "electronic cash" refers to services that contain monetary value in the products themselves and exist with the customer. The term "electronic payments system" covers a wide range of payments, including credit card purchasing, electronic check payments, and electronic cash.

Strictly speaking, the word "issuer" can be used only for those that create ("issue") electronic cash (e.g., DigiCash and Mondex), not for those that provide only credit card transaction services.

DigiCash. DigiCash was founded in 1989 by David Chaum, in the Netherlands. DigiCash sold Mark Twain Bank, based in St. Louis, Missouri, the license to provide "ecash" in the United States. "Ecash" is software-based electronic cash secured by means of encryption. With the "ecash" software, a customer withdraws "ecash" (a form of digital money) from a bank and stores it on a PC. The customer can then spend "ecash" at any merchant that accepts it. Person-to-person payments also can be performed with "ecash". Mark Twain Bank started issuing "ecash" October 23, 1995. DigiCash is expanding the service, and, Eunet Finland began providing "ecash" in March 1996. In May 1996, Deutsche Bank announced a joint pilot project with DigiCash; and in October 1996 Advance Bank of Australia announced it plans to issue "ecash" as well.

In the United States, "ecash" works in the following way. First, the customer signs up with Mark Twain Bank and opens an account. The customer obtains an application form from Mark Twain Bank's home page on the Internet. Because federal banking law requires the applicant's signature to open an account, the customer must send the signed form, along with the deposit money in the form of a check, wire, or money order, by ordinary mail to Mark

---

[5]Lynch and Lindquist, 29.

Twain Bank. Once the application has been approved and the deposit has cleared, the customer receives a personal identification (ID) and a password. With these, the customer can then download free software from the Internet to use "ecash." The bank charges a setup fee and also monthly charges, depending on balances.

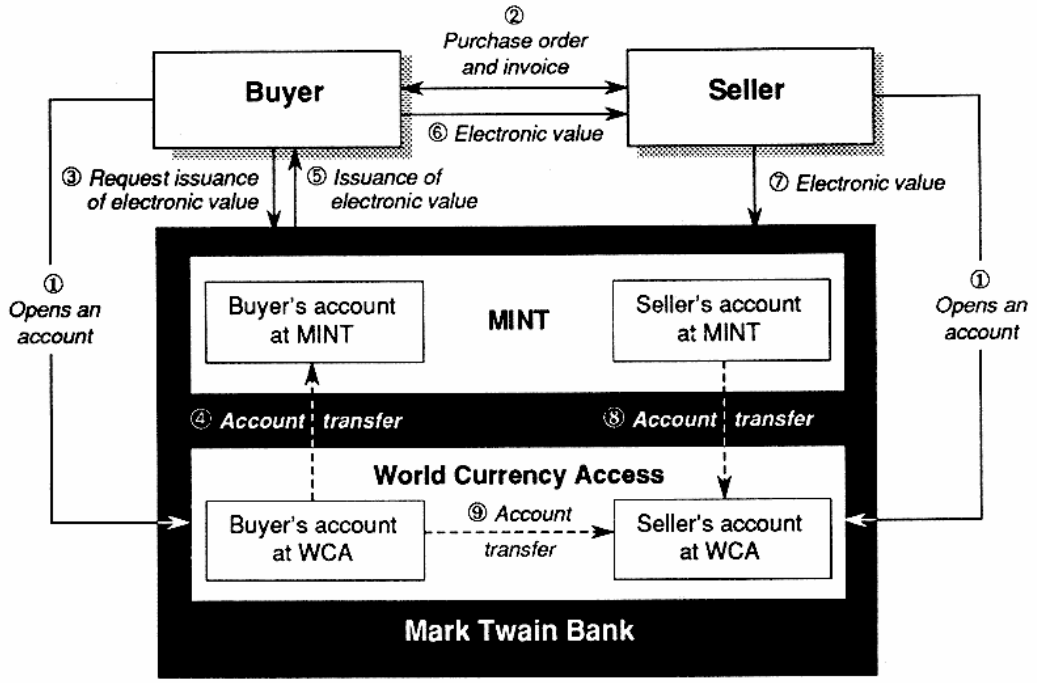
By opening an account at Mark Twain Bank to use "ecash," the customer is actually automatically opening two accounts. One is WorldCurrency Access (WCA), the other is "ecash Mint." Mark Twain Bank's WCA, like an ordinary bank checking account, is subject to the Federal Deposit Insurance Corporation (FDIC) requirements (up to $100,000), and the initial money from a customer is deposited here. Deposits can be made in twenty-five different currencies by check, wire, or money order, and there is no minimum amount for deposit. The money is then automatically transferred to "ecash Mint" (unless the customer specifically requests that the money be held at WCA), which the customer can download and keep on a PC hard drive to use for purchasing goods and services on the Internet (see **Figure 2-4**). Funds in the "Mint" are not insured by the FDIC and do not earn interest. There are three fee plans customers can choose from to set up "ecash": for less frequent users, the setup fee is U.S. $11 with a monthly fee of $1; for frequent users, the setup fee is $25 with a $2 monthly fee; and for heavy users, the setup fee is $25 with a $5 monthly fee. There is also a fee to move money back and forth between WCA and "Mint," and that fee varies according to the plan the customer has chosen.

Security is a concern with electronic cash. "Ecash" is secure, because it is anonymous and encrypted. It has its own note number (randomly determined by the customer's "ecash" software, not by the bank), which is assigned by the bank at the time of issuance in a way that makes it impossible for the bank to know what note numbers it has assigned. DigiCash also claims that "ecash" protects the payer's privacy by using a blind signature and strong cryptography. For example, when a customer asks to download $20 from the "ecash Mint," the bank sends the customer encrypted "ecash" in the form of an anonymous but secure transaction. (At this point in the transaction, the recipient of "ecash" is anonymous; the bank records only the amount of the deposit or withdrawal and the "ecash" serial number.) When the customer uses "ecash" to purchase service or goods, the merchant receiving the "ecash" transfers the purchase amount to the bank and the bank credits the merchant's "ecash Mint" account. The bank keeps track of numbers used or reported as lost.

According to Mark Twain Bank, if the same number is sent to the bank twice (one or both forged), the first number sent will be accepted.[6]

---

[6]For more about ecash security, see DigiCash [Homepage] [On-line]. URL: digicash.com/ecash/aboutsecurity.html



1. The buyer and the seller open World Currency Access accounts at the Mark Twain Bank.
2. A purchase order and invoice are issued.
3. The buyer requests issuance of electronic value from the Mark Twain Bank.
4. The value is transferred electronically from the buyer's account at WCA to the buyer's account at MINT.
5. Electronic value is transferred from the bank to the buyer.
6. Electronic value is transferred from the buyer to the seller.
7. Electronic value is transferred from the seller to Mark Twain Bank into the MINT account.
8. The value is transferred from the seller's account at MINT to the seller's account at WCA.

Source: Hitachi Research Institute.

Figure 2-4

Money Flow of DigiCash's "ecash"

A unique feature of "ecash" is payer anonymity. When paying with "ecash" the payer's identity is not automatically revealed to the merchant. The payer thus retains control of information. During a payment to a merchant, the payer can choose to be identified—but identification is by choice. The payee, however, is identified by the bank when the bank clears a transaction, which makes crimes such as money laundering difficult. Simply put, a customer can send "ecash" anonymously, but the bank cannot accept "ecash" anonymously.

DigiCash not only provides "ecash", but also has its own technology to develop smart cards; it is a leading developer in several European smart card projects. One of them is

CAFE, a consortium of electronic payments companies and research organizations, funded in part by the European Commission. CAFÉ, which stands for Conditional Access for Europe, is developing an electronic wallet to be used as a pan-European device for consumer payments, access to information services, and as identification. Together with the licensing of "ecash," DigiCash is capable of providing both payment on the Internet and smart cards.

2.2 Payment by Stored-Value Cards

2.2.1 Mondex

Mondex, developed jointly by NatWest Bank, Midland Bank, and British Telecom (BT), is a system that uses a smart card that can hold up to five separate currencies. The Mondex system aims to replace bank notes and loose change with smart cards. The card can store money ("Mondex value") and to transfer Mondex value from the customer's bank account to the Mondex card through ATMs or specially equipped telephones (i.e., public and home telephones with built-in card readers or a card reader that can be attached to ordinary home telephones). Once the value is in the card, the money can be used wherever Mondex is accepted. If the customer loses the card, the money in it is gone, just like a real purse or wallet. (The card can be locked with a personal ID number, so that a thief cannot benefit by stealing and trying to use it.)

An "originator" for Mondex value in each country acts as an issuer for the Mondex system. The originator issues Mondex value to participating banks and exchanges real money (i.e., legal tender) for Mondex value. Users of Mondex possess the Mondex card, a balance reader, and a device (called a "Mondex Wallet") that looks like a calculator and can read the customer's balances and even perform cash transfers. (The wallet has a higher function than the balance reader and performs cryptographic operations, can lock and unlock the card with PIN code, and acts as a viewer, for keeping track of the last ten transactions. The wallet contains an IC chip inside it, because communications and storage must be conducted with chips.)

If you wish to give your child some pocket "money," you slip your card into your wallet and first transfer into it the amount of money you wish to give your child, then slip your child's card into the wallet, enter the amount, and the value is immediately transferred. As of early 1997, a Wallet is in development that will accommodate two cards at once, easing transfers. Or, using a specially equipped telephone (or a card reader connected to an ordinary home phone), you could transfer value to a friend by phone if that friend also has special

equipment. Communication is direct, chip-to-chip; no bank or clearing agency intervenes.[7] As mentioned above, one unique feature of Mondex is that it is transferable and anonymous, just like cash. For example, merchants can use their Mondex values collected from sale of their merchandise for other payments. Mondex users can pass Mondex value to another user indefinitely, without the value being redeposited in a bank. In other words, Mondex value does not need to be settled at the bank each time one receives it. This anonymity enables Mondex value to be traced only when the user wishes to be revealed.

Another notable feature is that because Mondex is equivalent to cash, there is no need for the kind of verification needed with credit or debit cards. Off-line payments that do not need to identify the validity of the user make transactions less expensive than payments conducted on-line and are faster.

Mondex is not aimed at the Internet in particular, but those involved think the two systems are ideally suited for each other. By integrating the technologies of the smart card and the smart card reader connected to a PC, Mondex permits on-line transactions between consumers and merchants, consumers and banks, even consumer to consumer through PCs. This capability is still in development, and Mondex has not yet announced that it can provide such services over the Internet.

As of early 1997, Mondex is conducting several pilot tests around the world. The most famous is taking place in Swindon, England; it started in July 1995 and was originated by National Westminster Bank and Midland Bank. BT adapted 250 public pay-phones and made 2,000 home phones available for private use by consumers and retailers in Swindon, a town of around 250,000. As of February 1996, there were over 10,000 cardholders and 750 merchants involved in the pilot program. Mondex value is limited to £500 (about U.S. $800) per card, which is convenient enough to cover everyday expenses. Another test was begun in Hong Kong, in October 1996, backed by the Hong Kong Shanghai Bank (Midland Bank's parent), and another pilot in Guelph, Canada, with Royal Bank of Canada and Canadian Imperial Bank of Commerce, the two largest banks in Canada, as the originators. That pilot began in the first quarter of 1997. The California-based Wells Fargo Bank started a Mondex pilot in July 1996 in San Francisco, and approximately twenty-five retailers based near Wells Fargo's headquarters are accepting Mondex.[8] Another pilot was started in Australia and New Zealand, and some Central American and Southeast Asian countries are considering pilot tests. (Although Mondex is designed to carry up to five currencies, in each ongoing pilots only the national currency is issued.)

---

[7]"Burn Those Bank Notes—Digital Cash Is Coming," *PowerPC News* [On-line]. URL: http://www.ganges.cs.tcd.ie [ceased publication].

[8]Presentation by David Birch, Hyperion Systems Ltd., given at the Software Publishers Assoc. (Cannes, June 1996).

A notable feature of all these Mondex pilots is that each has interoperability with the other countries' pilots, and Mondex is aiming at a global de facto standard. In November 1996, MasterCard acquired 51 percent of Mondex, becoming the major shareholder. This acquisition indicates technology standardization is one step closer. Merchants have expressed concern about needing to acquire so many card-reading terminals, insert: one for each different card type. As of December 1996, AT&T Universal Card Services, Chase Manhattan, First Chicago NBD, MasterCard, Michigan National Bank, Dean Witter Discover (Novus), and Wells Fargo all joined together as purchasers of Mondex franchise rights in the United States. As of spring 1997, Mondex U.S.A is preparing to offer service.

Visa International. Visa International ("Visa"), the world's largest credit card company, introduced the technology of multipurpose prepayment cards for Danmont in Denmark and subsequently developed "Visa Cash."

A trial of Visa Cash was started in the Visa corporate office in California, and its use was later expanded to cover Atlanta on the occasion of the 1996 Summer Olympic Games. The target scale of the trial was issuing two million cards and the participation of 5,000 retail stores. The largest pilot experiment in a new electronic payments system, it drew attention from around the world. When the Olympic Games ended, the card remained usable at 1,500 stores of fifty participating retailers, most of them fast-food stores and gas stations. The total number of cards issued has not been disclosed. The three issuing banks were Wachovia Bank, NationsBank, and First Union Bank, all with a major presence in the southern United States. Two kinds of cards were issued: a rechargeable card purchased from banks and a disposable card purchased through vending machines.

In the trial of the rechargeable card in the head office, the upper limit of stored value was set at $100, but in the Atlanta trial the value set was entrusted to the issuing banks. The trial of the disposable card offered denominations of $5, $10, $20, $50, and $100. Visa Cash can be recharged from an individual's account through the ATM network, and the customer does not need to open a new account at the issuing bank.

With Visa Cash, consumers can spend the value on the card, but, unlike the Mondex system, the card cannot be used for payment between individuals. A Visa Cash transaction is made on the Visa financial network, so that all transaction data go through the data center of Visa International. The cost of the operation is relatively high, because all transactions must pass through the network for settlement process with banks.

Visa, jointly with another major credit company, MasterCard International ("MasterCard"), and with Europay, established the "EMV" (the acronym is based on the first letters of the three companies), a standard for some stored-value cards. In 1997, smart cards are expected, according to a current plan at Visa to replace current credit cards starting in the

Table 2-1

Major Electronic Payments Providers

Provider	Number of Customers or Cards Issued	Number of Merchants
CyberCash		
Cybercoin	NA	27**
Credit card	400,000*	100**
DigiCash		
Mark Twain Bank	10,000	37**
First Virtual		
(Aug. 1994–96)	173,918	2,523
Mondex		
England***	25,600	>700
Guelph, Canada	1,000	40
San Francisco (Wells Fargo)	700	22
Hong Kong	35,000 (signed up)	NA
New Zealand	750	NA
VISA		
Atlanta	>1 million	NA

* Includes CyberCash, CheckFree, CompuServe Wallets.
** As of February 1997.
***England = Swindon, Exeter, York.
NA = Not applicable.

Source: Data from World Wide Web Home Pages of organizations named. Table © 1998 President and Fellows of Harvard College. Program on Information Resources Policy.

United Kingdom, and global development of Visa Cash is being pursued at the same time. Testing has already started in Britain and Australia. Visa offers this service elsewhere, too; in Asia, Visa is allied with Standard Chartered Bank and the Bank of China, two of the three issuing banks in Hong Kong. In October 1997, Visa began to offer Visa Cash in New York City, in the borough of Manhattan, in a joint pilot of Mondex, Chase Manhattan Bank, Visa, and Citibank. Both Mondex and Visa Cash cardholders can purchase goods at participating merchants in Manhattan's upper West Side. This pilot has attracted attention for three reasons: first, it is the first joint trial of Visa and Mondex; second, the hope is that it will provide a more accurate barometer of everyday purchases than the Atlanta trial (which attracted mainly collectors and tourists); and, third, problems encountered at the Atlanta Olympics are now considered manageable (for example, merchants are given proper instructions on how to

operate card readers). The number of cards issued is expected to reach 50,000 customers, with 500 retail stores participating.

Visa plans to start services also in Japan; it started its first trial in Kobe, in October 1997, and plans to start a second one in Tokyo, in June 1998.

2.3 Other New Payments Technologies

Apart from the payment methods already mentioned in this chapter, there are other new movements in the payments systems field: Secure Electronic Transactions (SET), developed jointly by Visa and MasterCard, and Integrion. Both methods provide secure transmission to the user of private information, such as credit card number and account information.

SET is a joint technical standard protocol developed by Visa and MasterCard and was originally developed to transfer trade data over the Internet. A new advanced SET is being developed that will allow purchases made by using a credit card on the Internet to be safeguarded. SET is based on encryption technology from RSA Data Security and is designed to operate both on the Web and in a store-and-forward environment, such as e-mail. It is designed to permit banking software companies to develop software for their respective clienteles independently and to have them interoperate successfully.[9]

Integrion is not a technology but a private financial network created by IBM and fifteen banks. Initial members of Integrion are ABN AMRO, BANC ONE, Bank of America, Barnett Bank, Comerica, First Bank Systems, First Chicago NBD, Fleet Financial Group, KeyCorp, Mellon Bank, Michigan National Bank, NationsBank, PNC Bank, Royal Bank of Canada, and Washington Mutual. These banks represent more than half of the retail banking population in North America. Integrion hopes to start a pilot program in early 1997 and will provide secure, convenient electronic banking services over the Internet and other electronic channels. The goal is to establish an open standard for electronic commerce. Initially, Integrion will allow customers to execute all core banking transactions, such as balance inquiries, fund transfers, and electronic bill payments, and to send e-mail to their banks. Integrion aims eventually to provide electronic money and smart cards.[10]

---

[9]Marvin A. Sirbu, "Credits and Debits on the Internet," *IEEE Spectrum* **34**, 2 (1997), 26.

[10]"Home Financial Network, Inc., Announces Support of Integrion Coalition," Integrion Press Release, Sept. 10, 1996 [On-line]. URL: homenetowrk.com/news/printeg.htm

Company and Service	Characteristics		
	Definition	Payable Between Individuals	Anon
Cash on IC-Card • Visa International: *Visa Cash*	Multipurpose prepayment card with electronic "value" on IC chip	No	No (ca traced)
• National Westminster Bank: *Mondex*	Electronic cash	Yes (successive transfer is possible)	Yes
Cash on the Internet • Digicash: *e-cash*	Software money stored on the hard disk drive of a personal computer	Yes (difficulty in successive transfer because of inseparability of value)	Yes
• CyberCash: *CyberCoin*	Software money transferred between "virtual" accounts of CyberCash	Yes	No (tra
Check on the Internet • FSTC: *Electronic Check*	Electronic check for corporate use	No (only among companies)	No
• CheckFree: *CheckFree Payment Service*	Electronic check for consumers use (capable of settling for both ACH's and paper checks)	Yes	No
Credit Card on the Internet • CyberCash: *Credit Card Service*	Credit card payment by sending encrypted card number over the Internet	No	No
• First Virtual Holdings: *Internet Payment Service*	Credit card payment by sending ID number over the Internet	No	No
EFT on the Internet • Intuit: *Quicken*	EFT order over the Internet	Yes	No
• Cardinal Bancshares: *Security First Network Bank*	Direction of remittance over the Internet (currently limited between checking accounts and savings accounts of the same holder)	Yes	No

*Truncation: To send electronic data for remittance and to keep the checks at the acceptance, instead of transportin
ACH = Automated clearinghouse IC = integrated circuit EFT = Electronic Fund Transfer ID = ider
WCA = World Currency Access

Characteristics				Comments	
etween uals	Anonymity	Multi-currency	Security	Impact on Monetary Control	Miscellaneous
	No (can be traced)	No	Proprietary network and encryption	No impact (value is assured by checking account)	• Intended to reduce risk of money laundering and robbery • Maximum usable value under $100 • Historical data are recorded
ssive	Yes	Yes (up to 5 currencies)	Encryption, protocol, and TRM (data disappear during physical attack)	Originator can create credit technically, but monetary authorities can contol by restricting issuance to banks only	• Limit of card's value is preset (£500 in Swindon trial) • Card can be locked • System can be used on the Internet
ity in ause bility of	Yes	No (but WCA [real money accounts] accepts multicurrency)	Encryption	MINT can create credit technically, but monetary authorities can control by qualifying only banks	Limited on the Internet
	No (traced)	No	Encryption	No (value is assured by checking account)	
long	No	No	NA	Same as current check	Truncation* by image
	No	No	NA		
	No	Yes	Encryption	Same as current credit card	Close relationship with VISA and MasterCard in establishing SET protocol
	No	Yes	Payments by the ID number of First Virtual		There is a delay before merchants recieve payments because First Virtual holds the money received from customers in their account as reserve funds
	No	No	Protocol (SET)	Same as current EFT	*Microsoft Money* is similar
	No	No	Encryption		Aiming for full set of banking services on the Internet

ead of transporting them physically.
er ID = identification NA = not applicable SET = Secure Electronic Transactions TRM = Tamper Resistant Module

Table 2-2

omparison of New Payments System

Company and Service	Miscellaneous
Cash on IC-Card	
• Visa International: *Visa*	Intended to reduce risk of money laundering and robbery Maximum usable value under $100 Historical data are recorded
• National Westminster Ba *Mondex*	Limit of card's value is preset (£500 in Swindon trial) Card can be locked System can be used on the Internet
Cash on the Internet	
• Digicash: *e-cash*	Limited on the Internet
• CyberCash: *CyberCoin*	
Check on the Internet	runcation* by image
• FSTC: *Electronic Check*	
• CheckFree: *CheckFree Service*	
Credit Card on the Inter	lose relationship with VISA and
• CyberCash: *Credit Card*	lasterCard in establishing SET rotocol
• First Virtual Holdings: *In Payment Service*	here is a delay before merchants ecieve payments because First Virtual olds the money received from custom-rs in their account as reserve funds
EFT on the Internet	*Microsoft Money* is similar
• Intuit: *Quicken*	
• Cardinal Bancshares: S *First Network Bank*	iming for full set of banking services n the Internet

*Truncation: To send electronic
ACH = Automated clearinghous
WCA = World Currency Access

RM = Tamper Resistant Module

Table 3-1

Categories of Payments Through Cards

Payments System	Stored Value		Nonstored Value
Smart Card (with microchip)	Mondex (transfer of value; settlement with finality)	VISA (transfer of data; book entry transaction)	Cartes Bancaires (France)
Non-Smart Card (without microchip)	Telephone cards and transit cards using PET		Credit cards, debit cards, cash withdrawal cards with magnetic stripe

PET = Polyethylene Terephthalate

Source: Hitachi Research Institute.

Today, most smart cards are capable of only a single application, but when they will have multiple applications, as credit cards with stored-value functions to pay for small purchases and transit fares or as personal identification (e.g., driver's license), they will be truly valuable in everyday life.

The following comparison of the two kinds of SVCs is taken from *Overview of the Key Legal and Policy Issues Raised by "Electronic Cash" Technologies Under Existing Banking Law*, although not all examples from the original are retained here.[1]

a. Magnetic stripe stored-value cards (plastic or paper cards with encoded magnetic stripe)

(1) Closed system stored value card

(a) Single purpose card
(Example: mass transit cards, such as the Washington, D.C., Metro farecard system)

(b) Limited purpose card or Closed system
(Example: college cards for copying and cafeteria use)

(2) Open system or multipurpose stored value card
(Example: DANMONT, a Danish stored-card system that involves stored value card usable in vending machines, telephones, trains, buses, parking meters, and so on. Described in "The Electronic Purse"

[1]Thomas P. Vartanian and Robert H. Ledig, "The Federal Reserve Board of Governors Delivers Report on Stored Value Products and the Electronic Funds Transfer Act to Congress," 21st Century Banking Alert No. 97-4-14, April 14, 1997 [On-line]. URL: ffhsj.com/BANCMAIL/21STARCH/970414.htm

Chapter Three

Smart Cards

Because the United States, compared with other countries, is a network-based society, as of early 1997, it is possible for customers to make on the Internet. Anyone interested in opening an account at CyberCash, Security First Network Bank, CheckFree, or DigiCash can do so. But smart cards, such as Visa Cash and Mondex, are not yet available to the U.S. public (although Visa tested Visa Cash in Atlanta. during the Summer Olympics of 1996). In Europe, where "MEP" in Portugal and "GeldKarte" in Germany are the major examples of successful smart cards, the situation is just the opposite.

3.1 Definition of Smart Cards

Generally, the term "smart card" is used to mean cards with microchips that can store and recharge data or monetary value, or both, on them or sometimes cards with both a magnetic stripe and a microchip. A similar term often confused with smart card is the "stored-value card" (SVC). An SVC stores data or monetary value, or both, on a magnetic stripe or an IC chip, or both, and can be used to purchase goods or services. An SVC is a prepaid card with a magnetic stripe or a memory chip (or both) and with monetary value on it, but it cannot load new data. Smart cards that have microprocessors and can recharge data or monetary value have the functions of SVCs. For example, a $20 telephone card is an SVC because it has value on the card itself. Mondex is another example, because it contains monetary value on the card. On the other hand, credit and debit cards (in the United States) are neither smart cards nor SVCs, because there is no monetary value on the cards themselves. They are more like a payments instrument. See **Table 3-1**.

The definition of the nonrechargeable prepaid card and the value-rechargeable smart card is somewhat vague and confusing, but a function common to both cards is that they contain monetary value or data, or both. Cards with chips that contain only personal information often are also called smart cards, as in Germany, where every citizen is issued a health card that identifies the holder's insurance provider and account number. In a smart card resembles a credit or debit card in that embedded in it are one or more IC chips (not a memory chip but microprocessor).

In credit or debit cards, the value exists by the authorization given by credit or debit card companies through a private line (which is different either a telephone line or the Internet), not on the card itself. Smart cards have value or data on the card; they can be said to be cash (although not legal tender), which is both a weak and a strong point of this card.

3.2 Positive Factors of Smart Cards

In countries where credit cards are widely used by more than half the population, such as the United States,[2] smart cards may face difficulties in finding acceptance. Many people wonder what incentives there are for using them. Credit or debit cards already have a place in everyday life, but smart cards are different from those and can be considered both convenient and secure. Using the appropriate device, smart cards can, for example at any time and anywhere download money or data, saving the customer the time required to go to an ATM. Also, the customer can see how much is in the account either by using the device or through the Internet.

Positive features of smart cards for consumers include the following:

- *Instant account update:* Smart cards, such as Mondex, can be connected by using an electronic wallet, and the customer can keep track of the latest ten transactions.

- *Portability:* Smart cards can be used to download money from ATMs and from specially equipped telephones. One of their major purposes is to replace small currency, lessening the weight of one's wallet and reducing the costs of handling cash.

- *Greater security than traditional cash:* The sophisticated built-in encryption technology used in smart cards makes forging a smart card more difficult than color-copying a traditional bank note. IC chips are developed to be tamper-resistant.

- *Lower transaction cost for smart cards than for credit cards, and faster transactions:* The cost of a transaction for a smart card that works off-line and does not require verification by a bank at the time of use, such as Mondex, is lower than that of a credit card transaction, which requires verification. The money in the smart card will be verified in the merchant's POS terminal.

- *Remote transactions:* As in the Mondex case, remote transfer of money can be performed by using a specially equipped telephone or connecting an adapter to the phone.

- *Verification of card owner:* IC chips in smart cards can contain personal information, such as social security number and drivers license, which can be used to identify the owner of the card at the time of payment.

- *Ability to carry foreign currency:* The Mondex card can carry five currencies on one card. (Not all smart cards can carry foreign currency; Visa Cash can load only one currency on one card.) The customer preparing for foreign travel no longer needs to go to a bank for travelers' checks. Global use is a key feature of smart cards.

---

[2]According to the American Bankers Association, 63 percent had a general-purpose credit card in 1992. See "Banking Facts: Usage of General Purpose Credit Cards by Families: 1992" (1996), based on data from the Board of Governors of the Federal Reserve System [On-line]. URL: aba.com/usage.htm

Current Issues in Economics and Finance, Federal Reserve Bank of New York, April 1995.)

b. "Chip" stored value cards (also known as "smart" stored value cards). [Can also] have encoded magnetic stripe, but [do] have embedded integrated circuit or microchip. May be used for limited purpose or in open system.

Examples:

(1) Limited purpose: First of America Bank Corp. installed the first U.S. Bank-issued "campus card" at the University of Michigan and Western Michigan University in fall, 1995. The chip card, also with magnetic stripe, functions as an automated teller machine card, a SVC, and a building access/identification card. The stored value component work in campus vending machines, bookstores, laundry services and fast food outlets. The magnetic stripe acts as the ATM component and provides access to buildings, meal plans and other campus functions.

Students will load value on their cards by inserting cash into or accessing their First of America checking account via, CashChip stations located at the campus.... Merchants purchase or lease POS sale equipment. The university will pay for card manufacturing and for campus POS equipment. [See section **2.2.2**, for Visa International's "Visa Cash" and the Visa and MasterCard joint pilot in New York, in conjunction with two New York banks, Citibank and Chase Manhattan, which began testing use of Visa Cash and Mondex in upper West Side of Manhattan.]

. . .

(2) Open system: On July 3, 1995, Mondex U.K., a "chip" stored value card joint venture among National Westminster Bank, Midland Bank and British Telecom, completed its first electronic purse transaction (a newspaper purchase for the equivalent of $.45). The joint venture's test involves 1,000 retailers and 30,000 customers in Swindon, west of London. The joint venture has designed special automated teller machines and telephones and has built an electronic wallet for keeping track of electronic funds, for moving money from one card to another and for storing cash. The card can be "locked" in its wallet by punching in a code that renders the card useless unless it is unlocked.... [See section **2.2.1** for further information about Mondex.]

In the United States, noncash retail payments by consumers are made by check, credit card, or debit card. Thus, the U.S. has developed a highly efficient system of automatic check and credit card processing, which has proved to be a barrier to initiating and developing new payments instruments. The same can be said about Japan, where direct debit is widely used, along with advanced ATM networks. In Europe, consumers use a large number of checks (see **Table 3-2**), though not as many as in the U.S. Currency is less functional, i.e., one currency per country, although the "Euro" is supposed to be introduced by the turn of the century. The high cost of check processing is a serious problem, and in many countries domestic financial institutions have cooperated in popularizing and expanding bank POS (see **Table 3-3**). As a result, the use of bank POS (debit cards) as a payments instrument for individuals has spread, mainly in France, Sweden, Belgium, and the United Kingdom, forming a basis for generating electronic cash. Such expansion of POS networks in Europe means that European countries are a step ahead of the United States and Japan and many other countries in the development and use of smart cards (see **Table 3-4**). Most of the electronic cash promoted in Europe is in the form of SVC (multipurpose prepaid card) systems based on existing ATM and bank POS networks that use magnetic stripe cards and thereby allow the use of smart cards.

Table 3-2

Cheques in Developed Countries

Country	Cheques Issued (Millions)		Volume of Transactions per Person		Cheques Issued per $1 Million of GDP	
	1992	1993	1992	1993	1992	1993
Japan	350	328	2.8	2.6	94	76
U.S.	58,4000	60,297	228.6	233.5	9,671	9,460
Belgium	174	163	17.3	16.1	785	827
France	4,869	4,909	85.1	85.1	3,662	4,071
Germany	902	934	11.1	11.5	451	519
Sweden	71	51	8.2	5.8	290	271
U.K.	3,005	2,886	52.0	49.6	2,920	3,054

Source: Bank for International Settlements, Statistics on Payment Systems in The Group of Ten Countries, 1994. (Permission pending.)

Another reason for the wide use of smart cards in Europe is the statement made at the unification of European nations, declaring cost reduction of individual payments means a

All these features are not, unfortunately, present in all available smart cards. Consumers need to evaluate the various cards and service offering and choose which card to use, and smart card providers may need to add or refine card functions accordingly.

A notable move is occurring in the regulation of smart cards and SVCs. In the United States, the Federal Reserve Board has proposed an amendment to its Regulation E, which governs many electronic methods of payment, to cover certain SVCs and smart cards. The Board has proposed that cards that can store no more than $100 should be exempt from the provisions of the regulation. According to the proposal, a merchant would not be required to issue paper receipts when certain types of SVCs were used for payment, this change is likely to increase the use and convenience of smart cards and SVCs. In the Board's "Report to Congress on the Application of the Electronic Funds Transfer Act to Electronic Stored-Value Products" (April 2, 1997), the Board analyzed

> ...the effects of four different approaches for the wholesale or selective application of Reg. E to SV products, including: (i) requiring only initial disclosure of information concerning product characteristics; (ii) uniformly applying a subset of critical Reg. E provisions to all SV products; (iii) variably applying selected Reg. E provisions on the basis of products usage or characteristics; and (iv) variably applying selected Reg. E provisions on the basis of the underlying technology's ability to comply with regulatory requirements....
>
> [T]he Board's report suggests that it has left room to consider further the extent to which technological advances affect the products, protections and risk factors upon which Reg. E is based. For example, the extent that electronic signatures or encryption are used to authenticate transactions, the identity of certifying authorities, and the degree of protection afforded by a certificate nay be an important fact for consumers to know. Similarly, the increasing implementation of SV products as multiple-use cards may affect the disclosure, risk and notice features of Reg. E.[3]

3.3 Smart Cards in Europe

Smart cards are widely used in Europe. Europe's information and financial transaction processing system has evolved somewhat differently from that of the United States. Europe developed smart card technology as a cost-effective way to process transactions associated with various retail, telephony, and information retrieval applications.

---

[3]Thomas P. Vartanian and Robert H. Ledig, "The Federal Reserve Board of Governors Delivers Report on Stored Value Products and the Electronic Funds Transfer Act top Congress," 21st Century Banking Alert No. 97-4-14, April 14, 1997 [On-line]. URL: ffhsj.com/BANCMAIL/21STARCH/970414.htm

participating banks; and a nonrechargeable card for travelers or minors. The value-rechargeable card can load up to 400 Deutsche Marks (as of January 1998, about U.S. $ 220, with one DM roughly equal to U.S. $0.5557). GeldKarte can be used at participating merchants and at vending machines.

Table 3-4

Smart Cards in Europe

Project	Issuer or Player	Features
Danmont (Denmark)	Danmont (owned 50/50 by TeleDenmark and Danish Payment Systems)	Can be used at telephones, parking meters, vending machines, buses, trains, coin laundries, retail shops. Prices range from DKr10–200. Danmont issued disposable prepaid cards Sept. 1992; plans to issue reloadable cards in near future.
Avant (Finland)	Avant Finland	Disposable cards in use since Dec. 1992; reloadable cards introduced Feb. 1994. Cards can be used at kiosks, gas stations, transit systems.
Postcard/Postmat (Switzerland)	Ministry of Post and Telecommunications	Pilot project. Cards can be used in vending machines, telephones, and at fast food restaurants.
GZS (Germany)	German Banks and GAD, IBM, DBP (telephone companies)	Multipurpose card introduced 1993. Pilot project in Münster region.
GeldKarte (Germany)	All German banks	Electronic money feature added to exisitng Eurocheck card. Trial started March 1996.
MEP (Portugal)	SIBS	Trial use of electronic money for micro payments started 1992.
Proton (Belgium)	Banksys (ATM network company)	Examined specifications for electronic money beginning 1993. Trial started in mid-size regional cities 1995. American Express licensed for worldwide use.
Group Carte Bancaire (France)	Major French banks	Since 1992, every bank card in France contains a chip for cardholder ID and transaction authorization.

ATM = Automated Teller Machine
MEP = Multibanco Electronic Purse
SIBS = Sociedade Interbancaria de Servicos

Source: Mitsuru Iwamura, *A Guide to Electronic Money* (Tokyo: Nikkei Bunko, 1996), 26. Source for Group Carte Bancaire: Carol Hovenga Fancher, *IEEE Spectrum* (Feb. 1997), 53.

To use the GeldKarte system, a customer charges a unit of prepayment onto a GeldKarte card at an ATM (the amount is transferred from the customer's account to the bank's GeldKarte consolidated account and pooled with all other GeldKarte transfers). When

Table 3-3

Status of Bank POS in Developed Countries

Country	Number of POS Terminals per 1 Million Persons		Volume of Transactions per Person		Average Value of Transaction ($U.S.)	
	1992	1993	1992	1993	1992	1993
Japan	264*	168*	0.006	0.005	$97.7	$184.9
U.S.	450	759	1.3	1.7	24.0	24.0
Belgium	4,034	5,246	12.0	15.6	57.7	63.2
France	5,594	7,435	22.7	24.3	62.5	58.0
Germany	640**	344**	0.35	0.85	43.5	54.2
Sweden	1,640	3,054	5.3	7.2	101.0	67.1
U.K.	3,806	3,780	—	—	—	—

* Figures for 1993 and 1994.
** Figures for 1991 and 1992.
POS = Point of sale

Source: Bank for International Settlements, Statistics on Payment Systems in The Group of Ten Countries, 1994. (Permission pending.)

common purpose.[4] Since then, each of the European Communities countries has been seeking leadership in the development of an electronic cash system with a view toward eventual monetary union.

GeldKarte of Germany. In March 1996, Zentrale KreditausschuBder Kreditwirtschaftlichen Verbande (ZKA), or the Central Committee of Financial IndustriesUnion, started a pilot program in Germany for GeldKarte, a smart card program in which all German financial institutions participate. The pilot was restricted to the towns of Ravensburg and Weingarten near Lake Constance. At the end of 1996, program sponsors expected to expand the use of the GeldKarte cards nationwide.

GeldKarte is unique in that the electronic cash feature was added to existing bank cards, such as Eurocheck cards (which have multiple functions: used as ID when paying with personal checks; used to withdraw cash from an ATM; and used as a debit card), bank POS cards, and credit cards. There are two types of GeldKarte : a value-rechargeable card, connected to bank accounts, which require customers to apply for the GeldKarte at their

[4]See Commission of the European Communities, *Making Payments in the Internal Market, Discussion Paper*, Brussels, Sept. 26, 1990 (COM[90] 447 Final) (also known as the "Green Paper").

shopping at a retail store, the customer slides the GeldKarte card through the merchant's POS terminal, which verifies the card by data encryption standard (DES) encryption. After the card is verified, the amount of purchase is transferred to the merchant's POS terminal. The stored amount of payment is batch-processed at the end of each day and transferred to the merchant certification center. (There are two types of certification centers established for GeldKarte: one, established by financial institutions, registers unspent amounts of each card, and the other, established by merchants, checks and sorts payment data.) Notification of total payment is sent to the merchant's bank through the certification center, and settlement is made by transferring that amount from the pooled GeldKarte account of the customer's bank to the merchant's bank.

After the pilot test of two months, 50,000 GeldKarte cards were issued, 62.5 percent of which consisted of bank-issued cards in the pilot test region. Six hundred POS terminals were set up in more than 500 retail outlets. Within two months, the amount of value charged onto GeldKarte cards totaled 2.5 million DM (U.S. $1.4 million). GeldKarte plans to expand the service to wider applications, such as public telephones, buses, and taxis, and to other regions in Germany.[5]

MEP of Portugal. The Multibanco Electronic Purse (MEP) undertaken by the Sociedade Interbancaria de Servicos (SIBS) in Portugal is a good example of a typical smart card. SIBS was established in 1983 by twelve Portuguese banks to provide electronic banking services; thirty banks participate. SIBS operates on an ATM network (4,000 ATMs) and bank POS (40,000 POS terminals), making settlements and processing checks and direct debits.

In 1992, SIBS started the electronic purse project using a smart card, and in April 1994 the smart card service became available throughout Portugal. In this system, a smart card, called a MEP card, is issued by member banks to consumers, who use the ATM to charge a unit of prepayment on the card. That amount is transferred from a bank account to the deposit account of SIBS and pooled there. When a consumer shops at a retail store, the value of the purchase is transferred from the MEP card to a POS terminal at the retailer. The retailer then transfers the data to SIBS, which transfers value from the SIBS deposit account to the retailer's bank account.

---

[5]*Financial Information Systems*, 176 (September 1996) [Japan, The Center for Financial Industry Information Systems], 38-49.

Table 4-2

Comparison of Private Key and Public Key Cryptography

Type of Cryptography	Functions	Well-Known Encryption Systems
• **Private Key Cryptography**	***Drawbacks:*** • Secure channel needed for parties to agree on key and to transport key. • Each person using a private key needs his or her own unique key; hence, there is an enormous number of keys on the network. • Private key adds privacy, but not authentication.	DES, Skipjack, RC2, RC4, IDEA
• **Public Key Cryptography**	***Drawbacks:*** • Relatively slow. ***Advantages:*** • Wide dissemination of keys is suited to the Internet. • Security can be increased by combining with private key. • Provides authentication.	RSA, PGP, Viacrypt

DES = Data Encryption Standard
IDEA = International Data Encryption Algorithm
PGP = "Pretty Good Privacy"
RC2 = "Ron's Cypher 2"; Ron is Dr. Ronald Rivest, one of the three inventors of the RSA public key algorithm
RSA = Encryption system name, based on the initials of inventors, Rivest, Shamir, and Adleman

Source: *The Computer Lawyer* **13**, 5 (May 1996), 1-4.

The most commonly used encryption methods are RSA and DES. There are two groups of applications for encryption private-key cryptography and public-key cryptography (see **Table 4-2**).

DES is the most widely studied private-key cryptographic system. Jointly developed by IBM and the National Security Agency (NSA) in 1974, it was adopted as a Federal Information Processing Standard in 1977. DES works on 64-bit blocks of data and uses a 56-bit randomly generated key. There are 256 keys from which to choose. The use of triple-DES (DES used three times on the plaintext[2]) gives an effective 112-bit keyspace.[3] In general, the longer the keyspace, the stronger the cypher.[4]

---

[2]Plaintext is a message before it is encrypted.

[3]In cryptography, a key is a word that contains a certain number of bits. This number is called "keylength" or "keyspace."

[4]Edward J. Radlo, "Legal Issues in Cryptography," *The Computer Lawyer* (Aspen Law & Business) **13**, 5 (May 1996), 1-4.

Chapter Four

Important Factors in Promoting the Use of Electronic Cash

Certain issues cannot be ignored whether the service is payment on the Internet or by smart cards. To promote the use of electronic cash, it will have the following characteristics; see **Table 4-1**.

Table 4-1

Important Factors for Promoting Electronic Cash

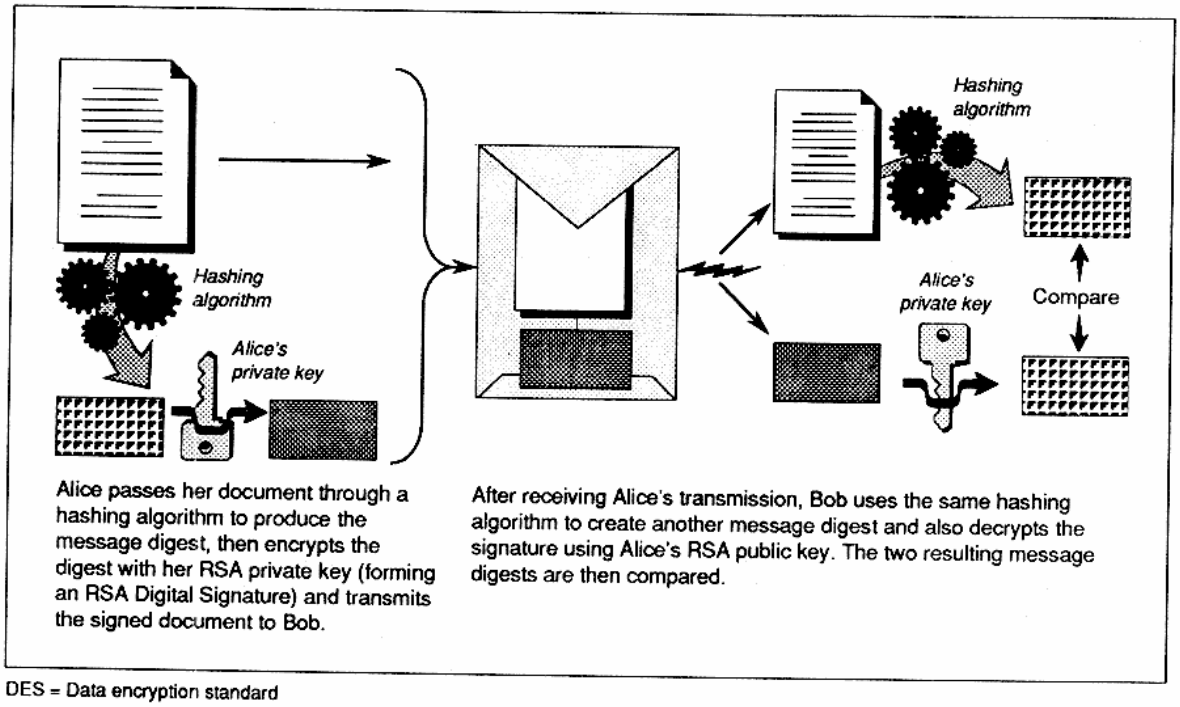
Secure transactions: • Prevent forgery, promote confidentiality: encryption • User authentication • Data integrity • Nonrepudiation
Choice of traceable or untraceable transactions
Development of trust among customers, merchants, and providers of electronic payment systems

4.1 Secure Transactions

4.1.1 Encryption

Encryption is the key technology for securing information placed on smart cards and for transmitting information over closed or open networks, such as the Internet. Cryptography technologies are the driving force for ensuring security, and major technology changes are made by nonfinancial institutions, such as RSA Data Security[1] and Nippon Telegraph and Telephone (NTT), for example. Because the security of data depends heavily on technology, the electronic payments market reflects an atmosphere of wait and see what's next. Reinforcing security means users can avoid both having their transactions read by others and forgery.

[1]The acronym RSA is used to the algorithm developed by Rivest, Shamir, and Adleman, whose initials gave it its name, and also to the technology and protocols they developed based on the algorithm.



DES = Data encryption standard

Source: Adapted from Steve Dussé and Tim Mathews, *EC.COM*, "S/MIME: Secure E-Mail for Electronic Commerce," September/October 1996, 36.

Figure 4-2

RSA Digital Signature

The whole issue of encryption policy was summed up in a question posed by Walter Wriston, former chief CEO of Citicorp/Citibank: "is the security of the world's financial network as important as communicating with SAC bombers?"[5]

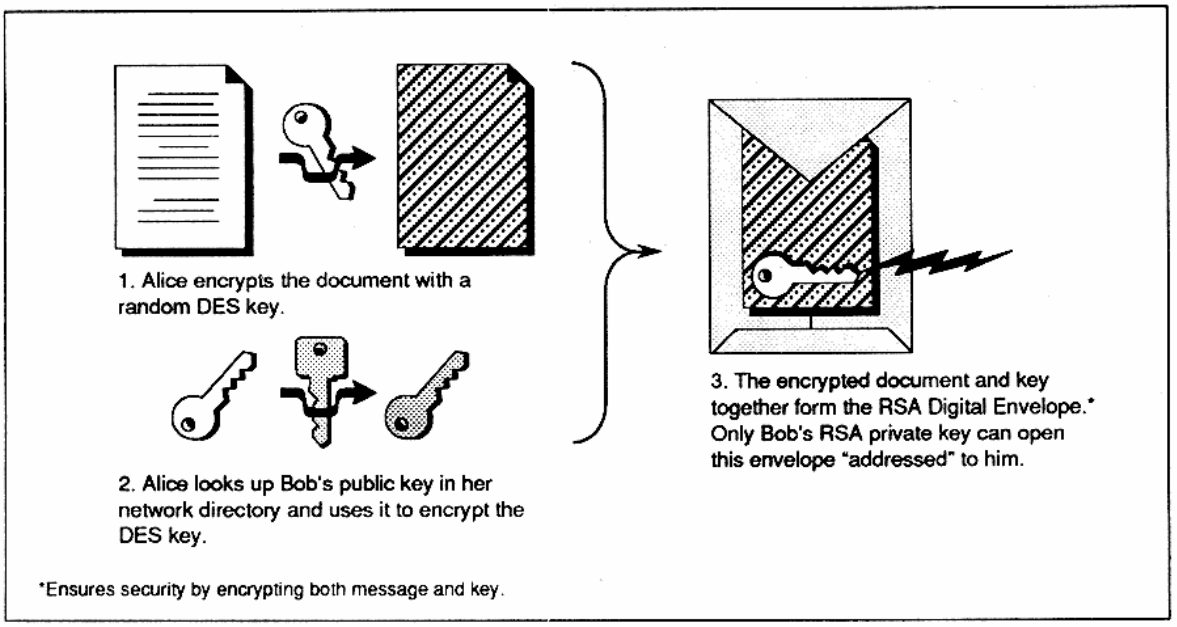
4.1.2 Authentication (Payment Authorization)

Many of the service providers of new electronic payments systems were initiated by financial institutions. Mondex, for example, was initiated by National Westminster Bank and Midland Bank; Security First Network Bank by Cardinal Bancshares; Visa Cash by Visa International. Backed by such institutions, these services offered customers assurance when providing electronic payments systems.

---

[5]Walter Wriston, quoted by Thomas A. Bass, in "The Future of Money," *Wired* (October 1996), 200. (SAC is the acronym for Strategic Air Command.)

The most commonly known and used public-key encryption was developed by RSA Data Security, founded by the developers of the fundamental algorithm, based in Redwood City, California. The RSA Digital Envelope provides message privacy, just as a mailing envelope protects documents inside from being read. To create the RSA Digital Envelope, a message is first encrypted with a secret key, such as DES or RC2, using a fresh, random key, which is then encrypted using the recipient's RSA public key. Typically, the public key is stored in the sender's "address book" or in a directory service. The RSA Digital Envelope consists of the combination of the encrypted message and the encrypted key. Because the recipient is the holder of the private key, only the recipient can open the Digital Envelope. See **Figure 4-1**.



DES = Data encryption standard
RSA = name of system and algorithm, based on initials of inventors, Rivest, Shamira, and Adleman.

Source: Adapted from Steve Dussé and Tim Mathews, "S/MIME: Secure E-Mail for Electronic Commerce," *EC.COM*, (Sept-Oct. 1996), 36.

Figure 4-1

RSA Digital Envelope

Another feature of RSA Data Security is the RSA Digital Signature (see **Figure 4-2**), which further enhances the security of information. Digital signatures are used to authenticate a message sent and to prove that it is original and has not been modified. Although effective encryption has offered hope of solving the problems of electronic cash, there is always a chance that computer systems can be broken into. Theoretically, cryptography, whether private or public key, is breakable. If the key is sufficiently large (i.e., has a large number of bits), then, given enough time, even the fastest supercomputer can break an allegedly unbreakable system.

reported on Certification Revocation Lists (CRLs), which list expired, revoked, compromised, or closed keys.

A trusted third party can serve as a CA, and the U.S. Postal Service is in the process of establishing a CA for the issuance of certificates. Verisign and GTE are leaders in CA services. Trusted entities such as the government, financial institutions, major hospitals, health maintenance organizations (HMOs), and telephone companies all have the potential to become CAs.

4.1.3 Data Integration and Nonrepudiation

Data integrity is important to prove that transaction data were not altered, either while in transit or in storage. Nonrepudiation prevents a sender from falsely denying having sent a message or having altered its contents.

4.1.4 Security of Smart Cards

The security and privacy of a smart card begins with strong encryption and tamper-resistant microprocessors. To enforce security further, the individual using the smart card is authorized to do so. This is "identification" issue. Identification measures should be provided at the discretion and desire of the payer, because in certain cases the payer may want to remain anonymous. "Identification" can be provided in a number of ways, such as by attaching a photograph of the card holder, registering fingerprints, hand geometry, DNA, digitized signature, or voiceprint onto the card. These security measures allow each smart card to be customized to the holder and connect card to the cardholder's identity.

Some experts believe that the current state of encryption technology does not offer adequate protection. Researchers at Bell Communications Research and two leading computer scientists in Israel, Adi Shamir (a professor in the Department of Applied Mathematics at the Weizmann Institute and one of the developers of RSA technology) and Eli Biham (a member of the faculty of Computer Science at the Technion), both have reported that discovering a way to decode encryption systems widely used in smart cards. They claim that private and public-key coding systems can be decoded if a computer processor produces an error and that heat or radiation can cause errors.[9]

Some promoters of smart cards, however, do not think this discovery will dampen enthusiasm for smart cards. Although no system can be considered completely secure, manufacturers are improving memory chips and microprocessors designed to protect cards

---

[9]John Markoff, "Two Israelis Outline New Risk to Electronic Data Security," *The New York Times*, Oct. 19, 1996, 37.

Electronic payments systems will not be useful unless both consumers and merchants trust them. Especially for payments systems in which new monetary value is transferred to the consumer, such as, DigiCash or Mondex, users must be able to verify that the money is authentic; merchants must be able to determine that the money was not counterfeited, and, according to Joseph R. Zimmerman, of Siemens, that it is backed up with value (as the gold standard backs up U.S. currency).

One way to assure consumers is to limit the issuance of electronic money to only financial institutions or institutions approved by the federal government that are allowed by law or regulation to receive deposits. Another way is to set up an institution for authentication that is respected by both buyers and sellers. "Trust" between buyers and sellers is essential in society, especially on the Internet, and authentication can be made possible by the use of digital signatures and digital certificates.

According to a report of the American Bar Association's Information Security Committee, Science and Technology Section; authentication is a "process used to ascertain the identity of a person or the integrity of a specific information."[6] Digital signatures and digital certificates[7] are used to authenticate the buyer (or sender of a message), and many believe these offer a foundation for Internet security. Digital signatures use public and private key pairs generated by the buyer (or sender). To reduce risk, the seller (or recipient) must be assured that the individual signing a payment order is who he or she claims to be. Digital signatures provide a function similar to that of a written signature, which authenticates the identity of the signer, asserting that the named person either wrote or agreed to the message to which the digital signature is attached.

Like passports, which certify the identity of citizens, digital signatures and digital certificates create the basis for a system of trust that incorporates the certification of key pairs by a party called a certifying (or certification) authority (CA) respected by both buyers and sellers. Digital signatures and digital certificates can be issued by a manager in a company, or any third party trusted by the buyer (sender) and seller (recipient). CAs must (1) be able to list or make public keys available and (2) have a method for revoking certificates if a public key becomes compromised or an account is closed.[8] Revoked public-key certificates are

---

[6]American Bar Association, Information Security Committee, Science and Technology Section, *Digital Signature Guidelines*, The Internet Council, October 1996, 28.

[7]A digital certificate is a digital ID card that connects a particular public key to its owner's identifying information, such as name, organization, and address. A digital signature is attached to the digital certificate, signed by a certifying authority, to verify the certificate's validity.

[8]Maggie Scarborough, National Automated Clearing House Association (NACHA), *Payments System Report*, June 1996, 1

IBM, the difference between key escrow and key recovery is similar to securing a house when its owner goes on vacation: instead of giving a key to two neighbors, the owner gives each neighbor half the combination to a lockbox that holds the key.

The conflict between the government on one hand and citizens and industries on the other remains largely unsolved (although some companies have agreed to participate in developing key recovery system: Apple Computer., Digital Equipment Corp., Groupe Bull, Hewlett-Packard, NCR, RSA Data Security, Sun Microsystems, Trusted Information Systems, and United Parcels Service). A balance between privacy and national security is difficult to achieve, and some parties will always be dissatisfied.

4.3 Development of Trust Among Customers, Merchants, and Issuers of Electronic Money

"Trust" among customers, merchants, and issuers of electronic money is important. Customers need to be assured that they receive goods (or services) they have paid for; merchants need to be assured that the customer is capable of paying for the goods (or services) and has valid electronic money; issuers of electronic cash risk having no one use their system unless it can be trusted. These degrees of "trust" may seem different, but without them the use of electronic money might cease.

Consumers must understand their responsibilities and rights in using electronic payments systems. Questions such as application of deposit insurance, where available, need to be addressed and under what conditions, and how, should electronic cash have the benefits of deposit insurance.

In the United States, the Federal Reserve Bank's Regulation E, which governs EFTs, provides consumers with specific rights and protections when using electronic payments. In April 1997, the Federal Reserve Board delivered a "Report to Congress on the Application of the Electronic Funds Transfer Act to Electronic Stored-Value Products" (April 2, 1997). Automated Clearing House (ACH) Rules and Regulations also outline detailed responsibilities of companies and financial institutions for electronic transactions.

Also in the United States, liability for fraudulent use of credit cards is limited generally to $50, if the consumer contacts the financial institution within two business days of the loss. Will a similar regulation accommodate payments on the Internet and by smart cards? In general terms, the Truth in Lending Act (TILA) "and regulations promulgated thereunder apply to consumer lending and obligate financial institutions to disclose and make clear to consumers the nature of credit transactions and the interest to be paid. TILA governs matters

from fraudulent access. Smart cards are actually more secure than credit or debit cards, because they have increased data security.

Concern about money laundering affects not only transactions using smart cards but also payments on the Internet. Tracking electronic cash going in and out of the country could be difficult. Government officials have expressed concern about electronic cash sent outside the country via the Internet. At the extreme, some believe smart cards with unlimited amounts could lead to disorder in the global financial system. To resolve these concerns in part, smart cards may need a safety feature to enable them to store up to only a certain fixed amount of value. As their use is intended to replace primarily small notes and coins, the cards do not need to store thousands of dollars.

4.2 Choice of Traceable or Untraceable Transactions

The issue of traceability is a difficult one, depending on who profits. Consumer groups insist that the value should be untraceable, in order to respect consumer privacy. From the issuers' point of view, however, the value should be traceable, in order to make replacement easier in case of loss or theft. From the merchants' point of view, traceable electronic money can be used to create customer databases of payments information, for sale to direct markets. In either case, consumers should be free to choose whether to remain anonymous. There are times when consumers want their identity clarified, such as when paying taxes, telephone bills, or utility bills. To avoid payments disputes, consumers should be able to choose whether to be anonymous.

There is a discussion surrounding the privacy of electronic money; the US government supports the idea of law-enforcement agencies being able to conduct electronic surveillance, such as decrypting encrypted messages, upon court authorization. This concept is called "key escrow." Those opposed to key escrow see it as a threat to invading citizens' privacy.

On October 1, 1996, the U.S. government said it would lift export restrictions on certain kinds of cryptography, provided that U.S. companies agree to cooperate in a procedure to give law enforcement officials access to the "keys" of such codes, on presentation of a warrant. As of late 1996, cryptography export is limited to 40 bits, except for financial transactions, which are allowed a 56-bit encryption key. It is commonly said that 40 bit is a low-level form of data scrambling and inadequate to protect against the increasing and increasingly sophisticated computer hacking.

Because "key escrow" has prompted much opposition from individuals and industries, a compromise system was to be implemented, a "key recovery" system, which U.S. companies are to develop by 1999. According to Kathy Kincaid, director of information technology for

such as finance charges, limitations on consumer liability for fraudulent use, billing errors, and other related matters."[10]

Providers of electronic cash need their responsibilities clarified, too. This new payments system may afford opportunities for nonbank organizations to provide electronic cash, and in the future many more companies and financial institutions may enter the service providers arena. Depending on whether issuance of electronic money will be limited to regulated depository institutions, this market offers great potential for every player. Those entering it need to be aware of both the character of the business—a public service to provide money—and of the importance of risk management. If for some reason an issuer were to go bankrupt, confidence in electronic cash might decrease, disrupting the financial market. To avoid such disruption, the issuer must make every effort to keep finances sound, and written law is needed to define issuers' responsibilities as well. Issuers of electronic money will need to disclose the contents of their services and products—such as transaction fees, whether consumers must pay interest in cases of delayed payments, procedures for resolving disputes and errors; and what happens if the product is lost, has expired, or cannot be used because of computer problems.[11]

---

[10]Ellen d'Alelio and John T. Collins, Steptoe & Johnson, *Overview of the Key Legal and Policy Issues Raised by "Electronic Cash" Technologies Under Existing Law*, Washington, D.C., July 31, 1995; quoting from Regulation 2, 12 C.F.R. Part 226.

[11]*The American Banker*, Oct. 24, 1996, 2.

5.1.2 Deposit Insurance

According to John D. Muller, an attorney at Brobeck Phleger & Harrison in San Francisco, the Glass-Steagall Act prohibits any entity from engaging "in the business of receiving deposits subject to...repayment upon presentation of a pass book, certificate of deposit or other evidence of debt, or upon request of the depositor," unless that entity is incorporated in the United States, permitted to engage in such business by the jurisdiction where the business is carried on, subject to examination by the banking authority of such jurisdiction, and publishes periodic reports of condition. 12 U.S.C. §378(a)(2). U.S. v. Jenkins, 943 F.2d 167 (2nd Cir. 1991) suggests that this statute is applicable only to individuals or entities that purport to be a bank or representative of a bank.[3]

Regarding deposit insurance, in General Counsel's Opinion No.8 issued in August 1996, the FDIC categorized the deposit insurance coverage of various types of stored-value products. The FDIC divided stored-value products into four types: (1) Bank Primary-Customer Account System; (2) Bank Primary-Reserve System; (3) Bank Secondary-Pre-Acquisition System; (4) Bank Secondary-Advance Systems.

The General Counsel's Opinion proposed that funds in the Bank Primary-Customer Account System appear to be insured deposits, while funds in the Bank Primary-Reserve System are not. It also comments that funds not received or held by a depository institution (Bank Secondary) do not qualify as insured deposits.

5.1.3 Consumer Protection

According to the CBO report, "Laws that protect consumers in financial transactions were passed in the late 1960s and early 1970s, partly in response to the increasing use of credit cards."[4] For the proposed new electronic payments systems, regulators and lawmakers are addressing such issues as consumer protection, disclosure and assignment of participant liability, and privacy. The outcome of amendments to existing regulations has still to be decided, and although the federal government has said it does not wish not to hinder the development of new payments methods, its stated wish to protect consumers makes for cautious progress in the development of amendments. As mentioned in the report prepared for the U.S. Department of the Treasury conference of September 1996:

> No body of transactional rules comprehensively defines the rights and obligations arising from electronic cash transactions. The gaps might be

---

[3]Glasser Legal Works, Second Annual Conference on "Emerging Law of Cyberbanking and Electronic Commerce," Little Falls, New Jersey, 137.

[4]CBO, "Emerging Electronic Methods for Making Retail Payments," 41.

Chapter Five

Regulation and Policy Issues

The report by the Congressional Budget Office (CBO), "Emerging Electronic Methods for Making Retail Payments,"[1] provides an organized overview of new electronic payments systems, in particular the regulatory framework. The report mentions that the advent of the new electronic payments methods raises a number of policy issues, some of which arise because current laws and regulations may not clearly cover new forms of payment. The issues include reserve requirements, deposit insurance coverage, consumer liability for unauthorized use, privacy of information about transactions, and state laws governing lost or abandoned financial instruments (escheat laws).

How the regulations will be applied to the new electronic payments systems will certainly affect the development of the market for them. Promoters of electronic money argue against imposing any regulations until the market for a new system has developed further. Several federal regulatory agencies (the Federal Reserve and the Office of the Comptroller of the Currency, for example) claim they do not want to hinder the growth of the electronic payments systems by regulating them at an early stage of development.

Clearly, many obstacles and challenges cloud the future of the electronic money business. As of February 1997, the federal government had begun to collect public opinion about applying parts of existing regulations to the new payments systems and about what new laws might be needed to protect consumers and avoid disruption in the financial market. The following is a summary of key issues.

5.1 Issues Concerned with the Regulatory Framework

5.1.1 Reserve Requirements

The Federal Reserve requires depository institutions to hold some fraction of checking and other transactions accounts in a cash reserve. Testifying before the Congress in October 1995, Alan Blinder, then Vice-Chairman of the Federal Reserve Board, stated that "under current regulations, stored value balances issued by depository institutions would be treated as transaction accounts and hence subject to reserve requirements."[2] The Federal Reserve, however, would have no authority to apply reserve requirements to balances issued by nondepositories.

---

[1]Congressional Budget Office, "Emerging Electronic Methods for Making Retail Payments," June 1996.

[2]Ibid., 40.

• Article 3 of the Uniform Commercial Code (U.C.C.) covers negotiable instruments and other commercial paper and is relevant to travelers' checks, nonbank money orders, and thus perhaps to "electronic money."

• Article 4 of the U.C.C. governs personal checks and other instruments payable by banks.

• Article 4A of the U.C.C. governs "wholesale" wire transfers (and not consumers).[6]

Federal Laws:

• **EFTA** (1978) and the regulations promulgated thereunder (e.g., **Regulation E**) govern transfers of funds through electronic terminals, telephone means, computers or magnetic tape authorizing or instructing a financial institution to debit or credit a consumer's asset account. In simple words, the Electronic Funds Transfer Act covers various electronic funds transfers involving consumers. The Act and regulations require disclosure to customers of the terms and conditions of such fund transfer agreements, set consumer liability for unauthorized transfers (generally $50), and establish rules on other matters such as delivery of physical receipts for transactions, error resolution and financial institution liability for technical malfunctions.[7]

• The Board of Governors of the Federal Reserve has been in the process of revising **Regulation E** (to the extent possible under the EFTA) to reflect more accurately the current state of the payments system and business environment. In May 1996, the Federal Reserve Board proposed changes to Regulation E that would recognize electronic communications as "writings,"[8] with certain conditions; and impose certain controls on stored-value card systems.[9]

• **The Truth in Lending Act (TILA)** of 1968 addresses some of the consumer protection issues raised by the use of credit cards. In general, TILA "and the regulations promulgated thereunder apply to consumer lending transactions and obligate financial institutions to disclose and make clear to consumers the nature of the credit transactions and the interest to be paid. TILA governs matters such as finance charges, limitations on consumer liability for fraudulent use (generally $50), billing errors and other related matters."[10]

---

[6]Henry H. Perritt, Jr., "Legal and Technological Infrastructures for Electronic Payment Systems," *Rutgers Computer and Technology Law Journal* **22**, 1 (1996), 45-46.

[7]Ellen d'Alelio and John T. Collins, Steptoe & Johnson, *Overview of the Key Legal and Policy Issues Raised by "Electronic Cash" Technologies Under Existing Law*, July 31, 1995, 16.

[8]For details, see section 4.1.2, on digital signatures.

[9]The Federal Reserve proposed an amendment to Regulation E, that stored-value cards in systems that do not track individual transactions would not be covered by the regulation. Other stored-value products would be covered to some extent by Regulation E, particularly in the area of initial disclosure requirements. SVCs of any type valued at $100 or less would be exempt. Ian W. Macoy, NACHA [On-line]. URL: nacha.org/reg_epro.htm

[10]d'Alelio and Collins.

> filled by contracts between the parties or by principles of law applicable to other payments systems that might apply by analogy. The rights and obligations of parties regarding risk allocation in electronic cash transactions thus may vary with the system at issue.[5]

Because the new electronic payments systems are not fully covered by current law or regulation, it will be left to participating parties to develop agreements and contracts.

Table 5-1

Types of Stored-Value Cards Identified by the FDIC

Bank Primary (Electronic value created by bank)	• **Customer Account Systems**: Funds underlying the stored-value card could remain in a customer's account until the value is transferred to a merchant or other third party, who, in turn, collects the funds from the customer's bank. • **Reserve Systems**: When value is downloaded onto a card, funds are withdrawn from a customer's account (or paid directly by the customer) into a reserve or general liability account held at the institution to pay when merchants and other payees make claims for payments.
Bank Secondary (Electronic value created by third party)	• **Advance Systems**: Electronic value is provided to the institution to have available for its customers. When customers exchange funds for electronic value, the funds are held for a short period and then forwarded to the third party. • **Pre-Acquisition Systems**: Depository institution exchanges its own funds for electronic value from the third party and, in turn, exchanges electronic value for funds of its customers.

Source: Information adapted from *Federal Deposit Insurance* [Home Page]. [[Page 40496]] URL: gopher.fdic.gov/division/occ/opd-comm.html

The regulations listed here are related mainly to forgery and privacy, which are big issues for consumer protection.

Regulations Related to Consumer Protection

State Laws:

[5]Staff, U.S. Dept. of the Treasury, *An Introduction to Electronic Money Issues*, prepared for the Treasury Conference "Toward Electronic Money and Banking: The Role of Government," Washington, D.C., Sept. 19-20, 1996, 41.

State Level:

- States, such as Utah (in May 1995), California (October 1995), Washington (March 1996), Arizona (April 1996), and Delaware (July 1996), have passed laws that give digital signatures the same validity as handwritten signatures. Similar legislation is pending in the states of Florida, Georgia, Hawaii, Michigan and New Mexico, and legislation is planned in Illinois, Massachusetts, and Oklahoma.

5.2 Issues Related to Policy

5.2.1 Effect on Monetary Policy

Electronic cash issued within the existing payments system will be under control of monetary agencies. According to Mark Bernkopf, of the Central Banking Resource Center, electronic cash will have only a minimal effect on the supply of money in advanced economies. For the next ten or so years, he said, economists estimate that electronic cash in the United States will make up only about 1 or 2 percent of M1, the narrowest monetary aggregate monitored by the Federal Reserve. Bernkopf mentioned that Central bankers fear widespread use of "person-to-person" transactions, which bypass conventional clearing systems, will reduce the ability of Central banks to monitor and influence the money supply. Central banks in other countries may find themselves threatened by electronic cash if the following three circumstances predominate:

1. Cash comprises a large proportion of the money supply (implying an economy with an immature financial sector).

2. Distrust of the local currency causes a flight to stronger currencies ("currency substitution" or "dollarization").

3. The country requires an advanced telecommunications infrastructure.In Bernkopf's view, "it is extremely unlikely that central banks will lose any substantial monetary power over the next decade. Though, this may very well change over the next 25 to 40 years."

5.2.2 Issuance by Nondepository Institutions

Whether nondepository institutions will be allowed to issue electronic cash is a basic question. If this were allowed, the question of the applicability of reserve requirements and deposit insurance coverage would come into play. Banks and other depositories may be at a disadvantage for issuers not subject to supervision and regulation.

According to Edward W. Kelly, Jr., a governor of the Federal Reserve, "the question of whether nonbank institutions should be allowed to issue electronic money is actively being debated in many countries.... [T]he Federal Reserve [has] concluded that any decision to

Most general bodies of commercial law address the risk of forgery, while addressing other risks. Forgery is universal topic and is relevant to any country, so all payments systems must accommodate a forgery defense and must identify the participant upon whom the risk of forgery falls.

The legal framework for conducting electronic commerce on an international basis is related to United Nations Commission on International Trade Law (UNCITRAL[11]). It is a model statute on EDI (electronic data interchange). The basic rule of UNCITRAL would be that the agreement of parties governs the transaction. As of late 1996, UNCITRAL is working on rules for government procurement contracts, "counter trade" (trades made in kind rather than in cash), standby letters of credit, and electronic funds transfers

Regulations Regarding Privacy

- **Fair Credit Reporting Act** enables an individual to sue any credit reporting agency or creditor for breaking the rules about who may see a person's credit records or for not correcting errors in his/her file.

- **Bank Secrecy Act of 1970**, also known as the Currency Transaction Reporting Act, was enacted to assist law enforcement in "criminal, tax or regulatory investigations or proceedings" by requiring banks, among other things, to keep records and file reports regarding certain large currency transactions.

- **Digital Signature Legislation.** Encryption and digital signatures are recognized as the key technologies to ensure the privacy and security of the message, and to prevent fraud. Digital signatures reduce the risk of repudiation and forgery. In a case of repudiation, a consumer may make a purchase using a payments system based on digital signature, then later fraudulently claim not to have made the purchase, that is, repudiate it. In a case of forgery, the purported purchaser says truthfully, "that is not my signature; it is forgery". Digital signatures are likely to provide technical solutions to forgery; and the laws that give legal effect to digitally signed messages are assisting the development of systems using digital signatures (see **Chapter Four**).

Federal Level:

- **Regulation E:** A draft of proposed revisions was released in May 1996. For the first time, Regulation E recognizes digital signatures in provisions addressing recurring electronic debits. Applying only to recurring electronic funds transfers, the proposed language recognizes that authorizations must be signed in writing or similarly authenticated, referencing digital signatures or code, and that they must be displayed in a viewable form.[12]

---

[11]UNCITRAL, created in 1966, has thirty-six members, elected by the General Assembly of the United Nations.

[12]Margaret Scarborough, *Security and the Internet*, Prepared for the Internet Task Force, The Internet Council, June 1996, 21.

5.2.4 Application of Tax

According to the CBO, the federal government has expressed worry that such illegal activities as avoiding income tax and sales tax may increase with the use of electronic money, particularly in systems that allow person-to-person (or computer-to-computer) transfers of value. Income tax may be difficult to determine and collect if payments come from anywhere in the world directly to a taxpayer's computer. Sales tax jurisdiction also may be difficult to determine, even in legitimate on-line transactions, because the relevant taxing jurisdiction may not know that a sale has occurred.[16]

[16]Ibid., 43.

reserve the nascent market for smart cards and other forms of electronic money as a province for banks alone might well stifle both competition and technological innovation in this area."[13]

A report by the American Bankers Association, *The Role of Banks in the Payments Systems of the Future*, concluded that only depository institutions should have direct access to the payments system, to reduce risk.

However, according to Henry H. Perritt, Jr., of the Villanova University School of Law:

> [I]f banking regulation does not cover the full range of issuances of money or quasi-money—as it obviously does not when one considers American Express traveler's checks, Seven Eleven money orders...the principal answer is that the legal system relies on the market, backed up by contract law. American Express traveler's checks are accepted because the market trusts that American Express will remain solvent. In other words, payments systems do not always look to the law to assure a fund for redemption; some systems are satisfied by the existence of a legal right against the issuer."[14]

5.2.3 Seigniorage

The CBO's report on *Emerging Electronic Methods for Making Retail Payments* defined seigniorage as the government's profit from the manufacture of coins. This profit is the difference between the face value of the coins and the cost of producing them. Seigniorage is the concern of the federal government's budget, and not of consumers. Wide acceptance of electronic money may have budgetary effects, because the federal government does not incur interest expense from public holdings of currency. If the new payments methods replace substantial holdings of coin and currency, the income to the government would be reduced. For example, according to the CBO report, in 1994 interest income from public holdings of currency amounted to about $20 billion, and the seigniorage on coins was about $700 million. If electronic money replaces 10 percent of the coin and currency in denominations of $10 and under, the government will forgo an estimated $370 million in interest and seigniorage per year.[15]

---

[13]Edward W. Kelly, Jr., at the Seminar on Banking Soundness and Monetary Policy in a World of Global Capital Markets, sponsored by the International Monetary Fund (IMF), Washington, D.C., Jan. 29, 1997.

[14]Perritt, 19.

[15]CBO, Emerging Electronic Methods for Making Retail Payments, 41.

Chapter Six

Stakeholders and Issues

Table 6-1 lists the major stakeholders in the electronic payments systems arena and their views on issues that arise with the new payments systems.

The new electronic payments systems are still in early stages of development, and their direction cannot yet be predicted. Many issues have yet to be overcome, and all stakeholders generally agree that barriers to the growth of these new payments systems need to be removed. The success of electronic cash will not be possible without cooperative efforts of government, industry, and the public, all joining to achieve these new and innovative payments systems.

Stakeholders	Anonymity	Electronic Cash vs. Traditional Cash	Issuance of Electronic Cash		
			By Government	By Banks	By Nonb
Government	Prefers traceable electronic cash to prevent forgery and money laundering	Seigniorage concern	The U.S. Mint proposed issuing stored-value cards	—	—
Central Bank	—	Effect of electronic cash on monetary policies "...will depend on amount and velocity... potential is greater than electronic bill payments"*		Edward W. Kelly: "...any decision reserve the nascent market for s cards and other forms of electron money as a province for banks a might well stifle both competition technological innovation in this a	
Commercial Banks	—	Electronic cash's handling cost is lower; faster transaction	—	ABA*** report: issuance should be limited to banks**	Concerned playing field
Other Financial Institutions (non-banks, investment firms, etc.)	—	Electronic cash may be a new product in competition against commercial banks	—		New compe product
Merchant		Reduces cost of handling cash	Provides assurance to merchants		
Consumer	Prefers choice between traceable and untraceable transcactions	Concerned about security, privacy, and fees	Provide assurance to consumers	Provide assurance to consumers	—
Electronic Payments System Provider	Mondex and DigiCash provide anonymous transactions	—	Limiting issuers of electronic cash may hinder free mark competition		
System Supplier Manufacturers (hardware, software)		New business opportunities	—	—	—

* Ernest T. Patrikas, First Vice President, Federal Reserve Bank of New York, "Regulating Commercial Activity on the Internet" [speech], Con
Mary & Westfield College, University of London, and UNISYS International Management Centre, *Federal Reserve Bank of New York* [Home
** Governor Edward W. Kelly, Jr., "Seminar on Banking Soundness and Monetary Policy in a World of Global Capital Markets, sponsored by th
*** American Bankers Association, *The Role of Banks in Payments System of the Future: A Report and Recommendations of the Payments Sy*
**** "Remarks by Chairman Alan Greenspan," Conference on Privacy in the Information Age, Salt Lake City, Utah, 7 March 1997, *Federal Reser*
FDIC = Federal Deposit Insurance Coproration POS = Point of sale

Ta

Stakehold

By Nonbanks	Tax Application	Deposit Insurance	Security		Other Issues of Concern
			Encryption	Authentication	
—	Concerned about tax evasion; question of applicability of tax	FDIC opinion: "Insurance coverage only if the value represented [is] linked to an existing deposit account"	Cryptography export control	U.S. Postal Service is certifying authority	
any decisions to market for smart ıs of electronic for banks alone competition and tion in this area."**	—	—	• High level of security needed for large payments • Alan Greenspan: "It is clear that security and privacy will be very important if confidence is to be established in these new systems"***		
Concerned about playing field	—	Depository institutions need to accept deposits	High level of security needed for large payments	—	
New competitive product	—	Insurance not required	High level of security needed for large payments	—	
		Deposit insurance will protect merchants	High level of security needed for large payments	Authentication is important to verify customer	Set-up fee; standardization of POS terminals
—	Concerned about double taxation	Deposit insurance will protect consumers	High level of encryption needed to enforce security	Authentication	
ler free market	—		Cryptography: major technology to enforce security	Authentication: important to enforce security	
—	—	—	Incorporating crypto-technology into products enforces security		

speech], Conference on Internet Banking and Payment: Regulatory Issues—A U.S. Perspective, St. Paul de Vence, France, 22-24 Jan. 1997, sponsored by Queen
w York [Home Page] [On-line]. URL: ny.frb.org/pihome/news/speeches/ep9070124.html
onsored by the IMF, Washington D.C., Jan. 29, 1997.
Payments System Task Force (Sept. 1996).
Federal Reserve Bank of New York [On-Line]. URL: bog.frb.fed.us/BOARDDOCS/SPEECHES/19970307.htm

Table 6–1

Stakeholders and Issues

Acronyms

ACH	automated clearinghouse
ATM	automatic teller machine
BT	British Telecom
CA	certifying (or certification) authority
CAFE	Conditional Access for Europe
CBO	Congressional Budget Office
CEO	chief executive officer
CRLs	Certificate Revocation Lists
DES	Data Encryption Standard
DM	Deutsche mark
EDI	electronic data interchange
EFT	electronic funds transfer
e-mail	electronic mail
EMV	Europay, MasterCard International, Visa
FDIC	Federal Deposit Insurance Corporation
FSTC	Financial Services Technology Consortium
GDP	gross domestic product
HMO	health maintenance organization
IC	integrated circuit
ID	identification card
IMF	International Monetary Fund
MEP	Multibanco Electronic Purse
NACHA	National Automated Clearing House Association
NTT	Nippon Telegraph and Telephone
PC	personal computer
PCMCIA	Personal Computer Memory Card International Association
PIN	personal identification number
POS	point of sale
RC2	Ron's Cipher 2
RPS	
RSA	Rivest, Shamir, and Adelman Company (and algorithm)
SET	secure electronic transactions
SFNB	Security First Network Bank

SIBS	Sociedade Interbancaria de Servicos
SVC	stored-value card
TILA	Truth in Lending Act
U.C.C.	Uniform Commercial Code
UNCITRAL	United Nations Commission on International Trade Law
WCA	WorldCurrency Access
WWW	World Wide Web
ZKA	Zentrale KreditausschuBder Kreditwirtschaftlichen Verbande (Central Committee of Financial Industries Union)