Electronic Cash

by Kevin P. Sheehan*

Credit-card issuers in the United States have begun to explore the idea of introducing electronic-cash products. Seven financial giants, including Wells Fargo, Chase Manhattan, and MasterCard, have agreed to market the Mondex electronic cash product in the United States.[1] VISA is developing a separate product. These products consist of a plastic payment card and other accessories, and consumers can use them to pay for goods and services the same way they use cash. Also like cash, consumers can use them for making person-to-person payments. These cards are equipped with microchips through which funds can be electronically credited and debited. Users transfer money from their bank accounts to their cards by inserting the card into an automatic teller machine (ATM) or a specially adapted home (or public) telephone.

Mondex maintains that its card offers consumers a number of benefits over traditional cash:

> It has an electronic locking system, which makes it more secure than cash, and it is also more convenient and accessible [it eliminates the need to carry coins and small notes, especially for routine daily transactions where exact change is needed]. Because of the similarity to cash, payment transactions do not involve authorizations or signatures. . . [Thus electronic cash is faster and easier than writing a check or getting a credit card authorization.] [W]ith Mondex it is [also] possible to carry out immediate [cash withdrawals] using specially designed pay phones, or private telephones providing customers with the convenience of a cash dispenser in their homes. (Mondex press release)

But Federal Reserve economist Harvey Rosenblum argues that "the current paper-based system doesn't have much to recommend it, other than it works great, is cheap, reliable, and we trust it" (quoted in Kutler (1997), 4). Mondex co-inventor Tim Jones disagrees:

> Physical money has problems. It can be lost, it can be stolen, and there are no records of cash transactions. You have to go to ATMs to get it . . . and you can't send cash to someone down a telephone line. Mondex overcomes these problems. . . . [U]nlike physical money, Mondex can be sent down a telephone line. And unlike money in a bank account there is no need to authorize a bank to make Mondex payments or to check that funds are available; there are no signatures to be validated or PIN numbers to confirm identities. Consequently there is no delay. As with a straight cash transfer, the recipient gets purchasing power instantaneously. (Quoted in Palmer (1994), 7.)

The dramatically declining cost of chip technology, plus the potential benefits to banks, retailers, and consumers, are leading to the widespread introduction of cash cards based on this microprocessor technology. Electronic cash systems are up and running in Denmark, Finland, Portugal, and Spain, while pilot projects are under way in several other countries. In fact, a high-profile New York City pilot is currently test marketing both Mondex and VISA Cash.

*Kevin P. Sheehan is a financial economist in the FDIC's Division of Research and Statistics.

[1]Wells Fargo will own 30 percent of Mondex USA; Chase will own 20 percent; and Dean Witter, AT&T, First Chicago NBD, Michigan National Bank, and MasterCard will each own 10 percent.

The sections below provide an overview of this new medium of payment, discussing the technology of electronic cash, the financial costs and benefits of moving to electronic cash, and the issue of consumer acceptance. An appendix explores the relationship between counterfeiting and electronic cash.

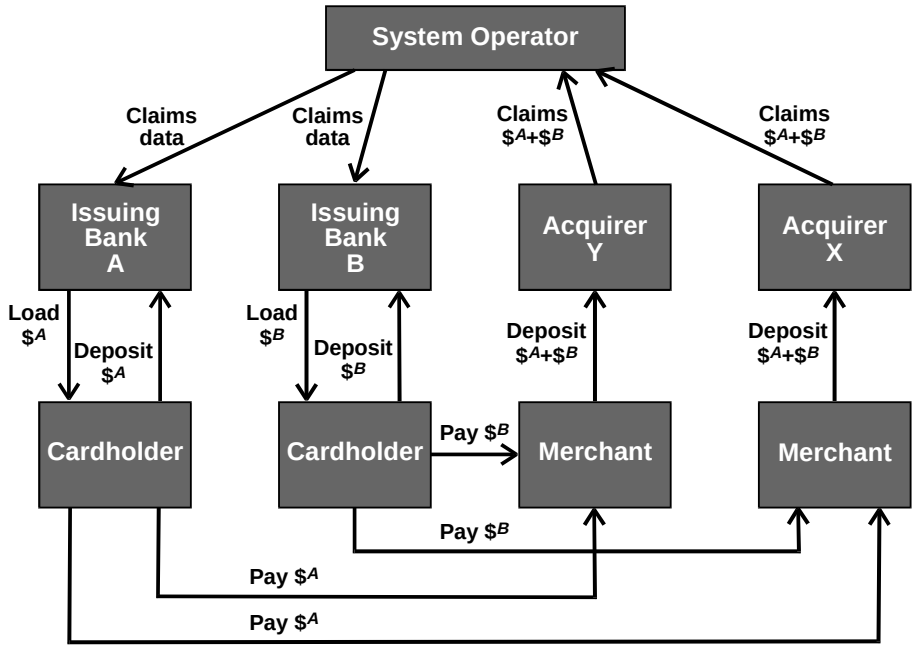
The Technology of Electronic Cash

The Bank for International Settlements reports that more than 300 billion consumer cash transactions take place in the United States each year, 270 billion of which are for amounts under $2. Soon banks will be offering a coin card with the capability to displace cash as the payment medium for a large number of these small transactions. These coin, or payment, cards are designed to be used in an open system composed of multiple card issuers, acquirers, and merchants. (Cards issued in an open system may be used to buy goods and services offered by any participating merchants. In contrast, cards issued in closed systems may be used only to buy goods and services offered by the issuing organizations. Washington's Metro farecard is an example of a card issued in a closed system.)

The transaction flow of an open system is illustrated in figure 1. Issuing banks provide cards to consumers, who load value onto these cards at specially adapted ATMs (Load $\$^A$ and Load $\$^B$ in the figure).[2] Consumers then use their cards at various designated merchants (Pay $\$^A$ and Pay $\$^B$ in the figure). At the point of sale, an electronic data-capture terminal records both the value of the purchase and the routing number of the issuing bank. At the end of the day, the merchant submits the entire batch of electronic cash transactions (Deposit $\$^A$ +$\$^B$) to his or her bank (Acquiring Bank), which forwards the electronic receipts to the system operator (Claim $\$^A$ +$\$^B$ in the figure). The system operator transmits these claims to the issuing banks, which then fulfill the interbank financial obligations resulting from the electronic-value transactions. When these interbank transactions are settled, the merchants are reimbursed by their banks.[3]

The coin card will be equipped with a microchip through which funds can be electronically credited and debited (see discussion below). Just as people now withdraw cash by inserting a card into an automatic teller machine, cardholders will transfer money from their bank accounts to their coin cards in the same way. This electronic purse will carry a running cash balance in its memory. Each time the card is used, the purchase amount will automatically be deducted from the card and credited to the merchant by an electronic reader. (Merchants will store their electronic cash receipts in specially adapted point-of-sale terminals, transferring accumulated balances to their banks at the end of the day by means of telephone links.) Payments will take just seconds. As with cash, no signatures will have to be validated and no personal identification numbers (PINs) will be needed to confirm identities.

Figure 1



$\$^A$: electronic cash issued by Bank A
$\$^B$: electronic cash issued by Bank B

[2]The figure illustrates a multiple-issuer system; however, a single-issuer system would work in the same way, also using multiple banks: the single issuer would create electronic value and issue it to participating institutions, which would then load this electronic value onto their customers' payment cards. Cardholders would use this electronic cash to make payments to merchants, who would later deposit these funds with their banks; this value would then be redeemed by the issuer.

[3]Notice that cardholders may make payments only to merchants, and merchants may clear these payments, or deposit accumulated balances, only through their acquiring banks. In other electronic cash systems, transferability is much less restricted. In systems like Mondex, cardholders are allowed to transfer value freely among themselves; however, merchants still deposit the electronic value received as payment.

Transactions will be conditioned solely upon the storage on the card of enough value to cover the payment.[4] The card is swiped through the electronic cash register and the transaction is completed.[5]

Current forms of electronic payment—credit or debit cards—cannot function as a cost-effective alternative for payments of very small value because of the costly on-line authorization process by which security is maintained. When a credit or debit card is presented at the point of sale, the merchant swipes the card through an electronic cash register that automatically routes a request for authorization to the bank that issued the card. This electronic cash register reads the cardholder's account information from the magnetic stripe on the back of the card and forwards this information, along with the purchase price, to the card-issuing bank. After checking the account number against a file of lost or stolen cards and verifying that funds (or credit) are available, the bank sends confirmation that payment is authorized.[6] This authorization procedure certainly enhances the security of the retail payment system, but the telecommunication costs of this on-line authorization process range from $0.08 to $0.15 per transaction, depending on volume.[7] These telecommunication costs generally preclude the use of credit or debit cards for payments of very small value.

Recently, however, credit and debit cards have begun to penetrate the $55 billion per year fast-food market, where speed of service has always been at a premium. To address this need for speed, card issuers have streamlined the authorization process. For transactions at fast-food establishments, the credit-card interchange "stands in" for the card-issuing bank and authorizes the transaction after first checking the cardholder's account number against a central hot-card file. If there is no match, payment is authorized and the amount is billed to the customer's account. Since there is no change and no sales slip to sign, the transaction actually takes less time than a cash transaction. But unlike cash, these transactions still require an on-line authorization using telecommunication services. Semi-off-line systems like those used in Europe and described below (see "Consumer Acceptance") economize on these telecommunication costs—without, however, being able to address the need for speed. Because the payor is required to enter a PIN at the point of sale, card payments in semi-off-line systems require more time than a cash payment

A cash payment does not require a telephone call or PIN. Nor do electronic cash payments. The technology at the heart of an electronic cash system (the one soon to be introduced in the United States, or any other) is a minute silicon chip, a microcomputer that is not only capable of storing information, presenting it, and transferring it to other, similar chips, but that also carries security programming. In other words, the microcomputer chips mounted on the backs of coin cards, and similar chips residing in electronic cash registers and automatic teller machines, can receive or store value or transfer it to one another and, more important, can authenticate the validity of transactions among themselves. As Tim Jones (co-inventor of Mondex) explains, "Every time value is exchanged, the two chips involved check that there has been no tampering with the transaction en route. [Chip] Number One says to [Chip] Number Two: 'I am a . . . member, are you?' And only if they both check out will they exchange value" (quoted in Palmer (1994), 7). This security, however, extends only to the value encoded on the card, not to the card's user.

For each transaction, the chip on the coin card releasing value and the chip in the electronic cash register accepting value confirm the authenticity of the other by examining the chip's unique "digital signature." The chip's processing facilities are used to implement a cryptographic algorithm. This algorithm generates a digital signature that must be authenticated by the receiving chip. This digital signature is the guarantee that the chips involved are genuine—or, more important, they guarantee that the signals have not been tampered with. The availability of funds is confirmed by the value stored on the card, and the authenticity of the electronic cash is confirmed by the digital signature that accompanies each electronic cash

[4]Given the anonymity of these payments, anyone can spend the electronic cash stored on a card. This anonymity exposes the cardholder to risk of loss—like cash in your wallet, electronic cash is lost if your card is lost or stolen.

[5]Most cards store and manipulate a numeric ledger, performing transactions as debits or credits to a balance. An alternative to these "balance-based" products is electronic notes. Electronic notes (often referred to as coins, or tokens) are issued in various denominations and stored on payment cards. In note-based systems, transactions are performed by the transferring of notes from one device to another. If a card does not hold the necessary denominations for a particular transaction, change is made by reconfiguring the notes on the card.

[6]Because of high communication costs, banks in Europe use a semi-off-line authorization process. Like cash, these systems economize on telecommunication costs. Credit and debit cards, however, also involve additional accounting costs. Monthly statements provide the cardholder with transaction detail for each payment. (If one were to use a credit card to purchase a cup of coffee each morning, then one's statement would detail each coffee purchase over the transaction period.) The bookkeeping cost of this record keeping is economized by the use of cash for those small transactions that need little documentation.

[7]*See* DePrince and Ford (1997).

payment. No on-line authorization using telecommunication services is required. (For a discussion of defenses against counterfeiting, see the appendix.)

Cost Savings and the Capital Investment

Electronic cash is starting to take off around the world because it eliminates the costs to banks and retailers of handling coin and currency. The U.S. Treasury estimates these costs at $60 billion annually in the United States (approximately $0.20 per cash transaction).[8] Electronic cash would limit these costs.

For banks, which provide the public with cash and therefore bear the cost of moving cash around the economy, an area of significant savings would be the cost of loading ATMs with paper currency. For retailers, there would be two areas of significant savings. First, because electronic cash receipts would be reconciled electronically and transferred over telephone lines directly from the store to the bank, sorting, counting, and transporting via an armored car would no longer be necessary. Thus, costs related to handling cash and coins would be reduced. Second, because electronic cash payments would not involve making change, retailers would not have to keep large amounts of coins and small notes on hand—thus, there would be little coin or currency to steal, and the security costs associated with robbery and employee pilfering would be reduced (perhaps the most important areas of savings for retailers). These potential savings alone explain why banks and retailers are willing to invest in such a capital-intensive cash-replacement technology.

Moving to electronic cash requires a large capital investment: payment cards must be provided to the public; existing ATMs must be replaced or retrofitted; and cash-only registers must be replaced by electronic terminals. But the cost savings should easily finance this capital investment.

Assuming only a 10 percent reduction of cash handling costs, cost savings over the next decade would be sufficient to finance a $24 billion capital investment. Approximately $2 billion of this total would cover the cost of providing payment cards to the public (the cost of payment cards runs somewhere between $2 and $10 apiece). From $1 billion to $7 billion would cover the cost of replacing the banking system's 150,000 ATMs (the cost of automatic teller machines runs somewhere between $7,000 and $50,000 apiece). Another $15 billion could finance the purchase of up to 30 million new cash registers (one new register for approximately every eight people, with the cost of terminals running somewhere between $500 and $2,000 apiece).

Consumer Acceptance

In late 1997, Chase Manhattan Bank and Citibank introduced electronic cash on the Upper West Side of Manhattan as part of a six-month trial. The pilot involves 50,000 consumers and 500 merchants, with Chase issuing Mondex cards and Citibank issuing Visa Cash cards. The test in New York is just one of many around the globe (Mondex has 16 pilots in 6 countries; Visa has 55 pilots in 17 countries).

These electronic-cash pilots have shown that the technology is effective, but they have also shown that, for the most part, consumer demand is lacking. Mondex, for example, was initially introduced in Swindon, a city of 100,000 located south of London. The first Mondex card there was issued in July 1995, and a nationwide rollout was anticipated for the following summer. Today, nearly three years later, Mondex in England is still issued only in Swindon, and only 13,000 cards are in circulation.[9]

One approach U.S. banks might use to address consumers' reluctance to accept the new payment instrument is to take an intermediary step and move to semi-off-line credit and debit operations, such as those currently used in Europe (see description below). Semi-off-line credit and debit operations are much less costly than the on-line system currently used in the United States. For this reason, banks in the United States are expected to move to a semi-off-line system using smart cards during the next few years. (Smart cards are payment cards equipped with a microcomputer capable of storing and processing information.)

A semi-off-line system as used by banks in Europe differentiates between large and small payments to economize on telecommunication costs. Large payments require an on-line authorization using telecommunication services, whereas payments less than the minimum large payment are authorized off-line. The payor simply enters an identification number at the point of sale, a number that must match the PIN stored

[8] *See* U.S. Department of the Treasury (1996).

[9] Although the Swindon experience is representative, a few electronic-cash trials have been successful. In the Ontario city of Barrie, more than 16,000 Visa Cash cards were issued in just three months; in the Ontario city of Guelph, approximately 10,000 Mondex cards were issued in nine months; a Hong Kong pilot that began in October 1996 has grown to 40,000 cards in circulation, with 5,000 participating merchants. For an overview of the e-money developments in more than 65 countries, see Bank for International Settlements (1997).

on the payment card; this PIN validation verifies card ownership. The availability of funds is then confirmed by a maximum charge limit also stored on the card. This limit is debited upon every off-line payment and is occasionally updated when the card is used with a POS having on-line capability.[10]

These payment systems do not impose a minimum size for off-line payments; thus, payment cards in these systems can be used for micropayments—that is, the purchase of newspapers, coffee, and other small-ticket items. But card payments in semi-off-line systems require more time than cash payments, since the payor must enter a PIN at the point of sale. For this reason, payment cards are generally not used at fast-food restaurants and other quick-service establishments. And for small purchases generally, consumers in Europe typically choose cash. A simple way of extending current credit and debit services into such transactions, however, is for banks to take the next step and load electronic cash on credit and debit cards, turning them into multipurpose payment cards. With these cards, consumers would use on-line payments for large transactions, off-line payments for small transactions, and electronic cash for micropayments.

Making micropayments with multipurpose payment cards would take just seconds. Payments would not involve a PIN or authorization at the point of sale; each time the card was used, cash would simply be transferred from the card to the merchant's terminal. When micropayments reduced the card's cash balance to zero, the cardholder would load more cash onto the card at the merchant's terminal. Electronic cash would be loaded in the same way an off-line payment is made: in each case the cardholder would enter a PIN, and the charge limit on the card would then be reduced by the amount of either the purchase or the cash withdrawal. For the cash withdrawal, the card's cash balance would increase by the amount of the withdrawal. At the end of the day, when the electronic receipt was returned to the bank, the cardholder's deposit account (or line of credit) would be reduced by the amount of the cash withdrawal. Cardholders would receive a statement at the end of the transaction period listing individually all card payments as well as the cash withdrawals. Note that off-line payments and cash withdrawals over the transaction period would reduce the card's charge limit.

Like making credit-card payments, using electronic cash stored on credit cards for small-ticket items would defer payment and carry benefits such as accrual of much-touted frequent-flier points. Alternatively, the technology of these payment cards would provide banks with a vehicle for paying interest on electronic cash stored on debit cards. When the cardholder loads cash onto the card, the bank will load an interest rate on the card.

For consumers, this multipurpose payment card would provide numerous benefits. It would give them "full micropayment capability, while freeing them from balance awareness, reloading hassle, and situations of insufficient cash" (Teicher (1997), 5). Use of paper currency requires trips to the ATM. In contrast, cards in an off-line system would function as remote ATMs by enabling the cardholder to load electronic cash at any merchant terminal, up to the card's charge limit.[11] These payment cards would offer consumers the services of cash without the inconvenience of a trip to the ATM.

Today no electronic payment system operates like the off-line system described above. In the system proposed by Teicher (1997), payment cards would function as remote ATMs, and electronic coins would be stored on payment cards and merchant terminals. When purchases reduced a card's cash balance to zero, more coins would be loaded onto the card from the merchant's terminal. But circulating electronic coins are not necessary in an off-line system—and in fact, they would introduce a problem endemic to paper currency systems: merchants would incur an opportunity cost, since they would have to keep some coins on hand for cash withdrawals.

The electronic cash described here would therefore be much more accessible than paper currency, and electronic-cash transactions would be faster and more convenient. Transactions would be faster because consumers would always have exact change—they would not have to wait for change at the point of sale. And for

[10]Banks in France use a semi-off-line system, and today nearly 90 percent of all card payments are authorized off-line. Moreover, since the implementation six years ago of this off-line system, fraud losses in France have declined by 50 percent (see Svigals (1998)). Payment in semi-off-line systems requires knowledge of a PIN that is stored on a tamper-resistant smart card. The tamper-resistant features of smart cards are aimed at protecting the PIN and other critical data from unauthorized observation. Given the secure storage of the PIN, fraudulent payments with stolen cards are virtually impossible.

[11]With payment cards functioning as remote ATMs, this off-line payment system would in effect make ATMs obsolete. With the proposed semi-off-line system, banks would be able to reap the savings of having fewer ATMs. Today there are approximately 150,000 ATMs deployed throughout the United States, and the monthly operating costs per machine run somewhere between $1,000 and $3,000 (see Belew (1997)).

transactions when exact change is required (for example, to board a bus or purchase something at a vending machine), electronic cash would be much more convenient. Still, consumers would use this electronic cash only if they expected it to be widely accepted.

Conclusion

Electronic cash is meant to be a substitute for a paper currency, and paper currency is universally accepted as payment. To function as an adequate substitute, therefore, electronic cash must have widespread acceptance. Current electronic-cash products have very limited acceptance. Electronic cash can be loaded on payment cards in semi-off-line systems because these systems employ smart cards that also function as coin cards, but such systems are not in use in the United States today. On-line systems, including the one currently used in the United States, use magnetic-strip cards that do not function as coin cards. For this reason, electronic cash cannot be loaded on U.S. credit and debit cards.

Given the current incompatibility between electronic-cash products and consumers' needs, products issued by organizations like Mondex must operate as stand-alone payment systems. In other words, Mondex (for example) must introduce its product retailer by retailer, and few retailers are currently equipped to accept its cash.

In contrast, if electronic cash were stored on a multipurpose payment card that had widespread acceptance, it would be usable wherever credit and debit cards were accepted. This electronic cash would piggyback on the worldwide network of existing retail card-authorization devices. By leveraging the widespread acceptability of credit and debit cards, electronic cash stored on a multipurpose payment card would offer the public a viable alternative to universally accepted paper currency.

APPENDIX

Counterfeiting electronic cash will involve the creation of payment cards that other participants in the system will accept as genuine—in other words, cards capable of replicating a digital signature. To duplicate a genuine payment card, one would need to procure a card with the same type of chip and load the appropriate operating system and application software. One would reconstruct the operating system and application software by examining genuine cards available through legitimate channels. These cards, however, are designed to prevent analysis and reproduction of the contents of the device. More specifically, physical barriers exist that prevent access to the application software stored on the chip:

> Tamper-resistant features of these [smart] cards are aimed at protecting data and software from unauthorized observation or alteration. . . . The software code resides in the chip and is designed to be protected from any external observation or modification . . . Such features make it extremely difficult and costly to observe or change critical data stored on the chip . . . or to alter the operating system or software applications. [This] hardware protection . . . includes physical barriers that prevent optical or electrical reading or physical alteration of the chip's contents. . . . Physical barriers also include external coatings as well as multiple layers of internal wiring that are very difficult to remove without damaging the chip itself. Active tamper-resistant features include sensors within the chip that detect unusual levels of heat, light and electrical current and render the chip inoperable under an attempted attack. (Bank for International Settlements (1996), 14.)

To date there have been no reports of security breaches of smart cards; nevertheless, "it can be assumed that even the most sophisticated tamper-resistant features may eventually be breached. . . . As a result, continued strengthening of the tamper-resistant features of card-based products will probably be necessary" (ibid., 22).

The tamper-resistant features of the payment card represent one of the most important security measures for electronic cash. But since these cards cannot be viewed as impenetrable, issuers must monitor their systems on an ongoing basis. In some cases, the security of electronic cash will be enhanced by the full accounting of individual transactions or the maintenance of cumulative records on individual devices. Alternatively, some systems will employ a value management strategy, which may be more manageable than full accounting. These systems will use a statistical analysis of transaction patterns. Procedures will be implemented to analyze system-level data on payment flows in order to detect unusual volumes of payments that could indicate fraud. Other methods to detect and contain fraud include the issuer's or system operator's periodic interaction by devices, and the hot-listing of suspect devices. Maximum balances and expiration dates on devices will also deter fraud as well as contain any resultant losses. Moreover, some systems will have the ability to change rapidly the cryptographic keys or algorithms used if widespread fraud is detected or suspected.

REFERENCES

American Bankers Association. 1994. Stored Value Cards: Technology and Implementation. *Payment Systems Strategies*. Summer.

Bank for International Settlements. 1997. *Survey of E-Money Developments*. Basle.

———. 1996. *Security of Electronic Money*. Basle.

Belew, Joe. 1997. Comment: ATM Fees Aren't a Rip-off but the Price for Convenience. *American Banker* April 24: 3–4.

DePrince, Albert E., and William F. Ford. 1997. The Privatization of Currency and Seigniorage. *Business Economics* 32 no.1: 25–32.

Kokkola,Tom, and Ralf Pauli. 1995. Electronic Cash. *Bulletin/Bank of Finland* 68 no. 12: 9–14.

Kutler, Jeffrey. 1997. Fed Officials Minimize Smart Card Potential. *American Banker* May 7: 4–5.

Palmer, George. 1994. Tim Jones: Mondex Mastermind. *Banking World* 12 no. 8: 7–9.

Schneier, Bruce. 1996. *Applied Cryptography*. John Wiley & Sons.

Svigals, Jerome. 1998. Comment: Behind Smart Cards Lie Chances for New Revenue Growth. *American Banker* January 15: 13–14.

Teicher, Mordechai E. 1997. *Reestablishing the Business Case for Stored Value*. Ultimus Ltd., Kfar-Saba, Israel.

U.S. Department of the Treasury. 1997. *An Introduction to Electronic Money Issues*. Washington, DC.