DIGITAL CASH

The Future of Digital Cash

by Karsten Schulz

The development of the Internet has paved the way for innovations in the payments system. There has been much speculation about the "superseding of cash," a "revolution of the monetary system," and the transition to a "cashless society" resulting from these innovations without considering the features and implications of these "e-money schemes."

The question is to what extent will these technical innovations in the payment system change the way society uses cash?

This article describes "electronic money" and its relation to existing payment systems. The article concludes with a look at some payment systems "under construction," which are expected to have far-reaching effects on the use of cash and the monetary system.

The Functions of Money

"Money is what money does."[1] This trivial description characterizes money according to the function it fulfills. Any asset that serves as a means of payment, unit of account, or store of value represents money.

Forms of Electronic Money

The existence of interrelated computer systems means that a variety of non-cash means of payment are available. These electronic means of payments share key commonalties. Payments are submitted electronically, and both payer and payee must hold an account at a bank. These systems make it possible for users to conduct transactions electronically on the net. Electronic fund transfer (EFT), credit and debit cards are examples of such systems. These electronic payment systems could be grouped under the "e-money" heading, regardless of whether executions are carried out over the Internet. However, the economic principle that underlies the creation and use of this book money remains unchanged. It should be noted that "immaterial" or cashless transactions are rising as a percentage of the total volume of payment transactions. Measured by overall value, transactions on the Net significantly exceed simple cash transactions. The monetary consequences resulting from e-money systems arise primarily from its potential to replace cash. Because these systems are not able to assume all the functions of cash, it is not likely they will replace traditional notes and coins.

The monetary consequences resulting from e-money systems arise primarily from its potential to replace cash.

From an economic and political point of view, payment systems that attempt to produce an electronic replacement for cash (namely "digital cash") are of much greater interest. Like traveler's checks or private bills, however, this "digital cash" (issued by private financial institutions) is not legal tender but rather a claim against the issuer. The redeemability of these claims is regulated by contract.

E-money systems that realize the potential of this concept are based on smart card systems or software solutions on the Internet. These systems may be combined to create digital money. Both systems do not necessarily need the connection to a bank account to initiate payment transactions. Credits are saved on smart cards or hard disks and can be transferred between these media directly, without an online connection to a bank account.

Smart Card Systems

The purpose of smart card systems was to provide a cost-saving medium for replacing cash in low-value

Karsten Schulz is a research and teaching assistant at the Heinrich-Heine University Duesseldorf, Department of Economics. Email: <*schulzk@uni-duesseldorf.de*>. A webpage containing the links referred to in the article is maintained by the author at: <*www.wiwi.uni-duesseldorf.de/vwlth/schulz/*>.

purchases and at unattended points-of-sale. Smart cards are expected to have advantages over cash in terms of comfort and the transaction costs associated with transfer, storage, transport and security of funds. Smart cards can perform a variety of other functions, such as the storage of social security and health care information or information related to a merchant's loyalty scheme. Smart cards also have cost and functional advantages vis-a-vis debit and credit cards, for example, lower costs for a single payment transaction, the finality of face-to-face and non-face-to-face payment transactions, and higher anonymity[2].

The major disadvantages of smart cards replacing cash include the necessity of a hardware installation, lack of the status as legal tender, lower anonymity, and uncertainty concerning security. These issues must be resolved, and users need to be convinced that smart cards are a value-adding solution.

Mondex

The Mondex system was originally developed as a smart card system. It is one of many smart card-based digital cash systems,[3] but its technical specifications make it an extremely close substitute for cash. Mondex's goal is to create an "electronic equivalent of cash."[4] The MasterCard-owned Mondex system has a microprocessor implanted on a plastic card serving as memory for the digital money.

The money, cryptographically marked and brought into circulation by the "originator," is available for various payment purposes. The electronic units of value are sold to the public by financial institutions against a legal means of payment and are redeemable at any time. Bank customers download Mondex value onto their cards before making a payment. In contrast to debit and credit cards, Mondex does not include any credit facility for the customer. In effect, loading the card represents an interest-free loan from the consumer to the bank.

All Mondex cards are electronically labeled so that the bank can assign an account to every card issued. As the identification of the card is transferred with every transaction, and the most recent transactions are stored on the card, the bank can trace the card's transactions. The number of stored transactions is adjustable and depends on the storage capacity of the chip. Because the card is not tied exclusively to a single person, the bank is not able to determine the user. This means that although there is a larger degree of anonymity compared with traditional credit card transactions, Mondex does not achieve the level of anonymity provided by cash transactions.

Although there is a larger degree of anonymity compared with traditional credit card transactions, Mondex does not achieve the level of anonymity provided by cash transactions.

Value can only be transferred from one card to another; this is done by reducing the stored amount of Mondex value on the payer's card and crediting the payee's card.

With the Mondex system, it is not necessary to perform an online check of the card or use third parties. The payee does not have to assume the risk of an "uncovered" payer's card, as the transaction is executed immediately (if sufficient Mondex value is stored on the payer's card). Because Mondex is a so-called "offline electronic cash system," it requires extensive security efforts to keep the system closed. This is achieved by advanced encryption techniques, branding of cards, recording of transactions and transaction analysis after reflow to the bank. The security system automatically changes if any fraud or manipulation is detected. Here the trade-off between high anonymity and maximum security takes shape.[5]

The difference between the Mondex system and other smart cards is its ability to perform peer-to-peer digital money transactions without a check from the issuing financial institution. This means that the stored money is an anonymous negotiable owner claim on Mondex—literally privately issued digital cash. This distinguishes it from "analog" cash, which is an uncovered claim against a government institution that can not go bankrupt because it can create the medium of redemption itself. Further, Mondex money is not insured by the Federal Deposit Insurance Corporation (or comparable institutions in other countries), as it is not tied to a bank account.

In sum, it is clear that Mondex money cannot take over all cash functions. In particular, there are anonymity and security concerns which could "hold up the show."[6] Nevertheless, features like multi-functionality, cost diminution and suitability for non-face-to-face payments could overshadow these disadvantages and promote widespread use of Mondex or a similar system.

Mondex did not have the success and acceptance of its smart cards in previous field tests, presumably due to the above-described weaknesses. Mondex plans to add two features to the system to make

Mondex superior to "analog" cash: multifunctionality and suitability for use on the Internet.[7]

Driven by technical progress in the field of smart card chips and advances in encoding technology, Mondex hopes to expand its functionality by "renting" storage capacity on the chip to third parties (MULTOS[8]). The user decides what additional functions he or she would like to load on the smart card. At the same time, the development of Mondex for home banking and payments over the Internet will satisfy the increased need for developing a payments system for Internet transactions.

Although it was initially intended to replace small cash transactions, Mondex has evolved to a position from which it can challenge the use of "analog" cash. The next step is logical—the design of a multifunctional payments system with worldwide availability. Mondex is no longer competing solely against cash. It now competes with other forms of electronic money as well.

Software Based Systems

Many e-money schemes designed for the Internet are nothing more than encoded procedures for the transmission of credit card or check information over the Internet (and therefore connections to traditional bank accounts). This is not what is meant in this discussion of "digital money." Simple check and credit card payments do not meet the special needs of an Internet payments system, are too expensive for small transactions, and can not be used anonymously.

Although it was initially intended to replace small cash transactions, Mondex has evolved to a position from which it can challenge the use of "analog" cash.

The economic incentive to issue private (electronic) currency lies in the issuer being able to borrow interest-free from the users. Debit and credit cards do not offer an opportunity to earn seigniorage. Instead, the economic incentive is derived from the ability to charge fees for the mediation between bank accounts. The user must decide if the fees of credit card payments are higher than the opportunity costs for prepayment of digital money. Functional advantages of digital money, such as anonymity and the finality of the payment transaction must be taken into account. It must be determined if e-money schemes designed for Internet payments (and payment systems that use the Internet to get around state controlled monetary systems) can win market share.

eCash

The technology created by DigiCash comes closest to realizing the concept of a cash equivalent for the Internet. The starting point of money circulation is an "eCash-account" for every customer at the issuing bank. Issuing banks receive the eCash token from the "mint." The customer then fills this account with digital currency directly from a traditional checking account.

Using special software, the user loads digital "one-way-money" (labeled with a digital signature and a serial number) into an electronic purse on the hard drive of his or her PC. This procedure is similar to the Mondex system. If the customer wants to pay for goods or services with eCash, an online check is initiated over the Internet to verify whether the token's digital signature is valid and to ensure that the token has not been used before. To detect deceitfully copied tokens, the eCash coins offered for payment are compared to the database of spent coins stored at the mint.

After the payee receives confirmation from the bank that the offered eCash has not already been spent, the payment is accepted, the eCash value is credited to the payee's eCash-account at the bank, and the used coins are added to the database of "spent coins" at the mint. This procedure takes place within seconds. ECash payments are not limited to retail transactions or shopping in cyberspace; they can also occur between private individuals. Because the online connection operates over the Internet–in contrast to credit card authorizations–eCash is accessible to all people, without requiring additional hardware. Because every eCash coin can only be spent once, a payee must download new tokens from his eCash-account to use them for future payments.

The uniqueness of the system lies in its exceptional commitment to user anonymity. DigiCash inventor and founder David Chaum says an electronic payments system for the Internet must reflect the character of the Internet. Technically, this is realized through the use of "blind signatures" that neither the mint nor the bank can trace to a person or entity.

In contrast to the Mondex system, cash-like anonymity is achieved. It is reasonable to expect that anonymity will remain important to DigiCash. This is even more remarkable given that, unlike Mondex, DigiCash's technology is software based. The security concerns related to software-based systems

as compared to smart cards with "tamper-resistant" hardware is that the software-based systems must include an online check.

It appears that the first major field test with eCash did not have the desired results. The Mark Twain Bank, the only US pilot customer, allowed its pilot test involving 5,000 customers and 300 storekeepers to end September 14, 1998. Two months later DigiCash announced "that it is entering into a Chapter 11 reorganization to allow it to pursue strategic alternatives for its electronic cash (eCash) products."[9] This seems to legitimize the question of whether the eCash system is ideally suited for the US market. A payment transaction with eCash requires that both payer and payee hold an account at the issuing bank because the one-way eCash token must be returned to the clearinghouse. This seems impractical for the decentralized US banking system. Field tests in Europe and Australia might have greater chances of success because the banking systems in these regions are more centralized. Also, consumers in Europe have generally had more experience with prepaid payment instruments.

Another obstacle to the widespread use of eCash lies in its confinement to Internet usage. DigiCash needs to extend its system to include off-line payment transactions. "Future extensions such as the extension to offline eCash, where the use of smart cards and the Internet are combined into a highly versatile and secure privacy-protecting payment system"[10] are in the pipeline. Mondex and DigiCash appear to be heading in the same direction: issuance of a private currency which not only replaces cash for traditional payments but also brings the concept of cash payment to the Internet.

Both systems will profit from technological improvements, particularly with regard to transfer, storage, and cryptographic techniques. Changes within existing technologies are also possible. The traceability of payment transactions, the linking of digital cash to bank accounts, and the redeemability of issued money into legal tender are some issues that need to be addressed.

"New" Currency Systems

Facilitating the redeemability of digital cash for legal tender would prepare the way for a "new" monetary system. All traditional and new electronic means of payment have attempted to challenge cash. Digital cash appears to have the potential to succeed and might – in the extreme case – replace notes and coins. However, in the e-money schemes described so far, digital cash represents nothing but a redemption claim against the uncovered government-issued base money. The clearing deposits of commercial banks on the books of central banks (*i.e.*, government controlled money) will survive[11] and the quality of government money as a store of value will still be adopted by digital cash.

Over the last two years, many currencies, such as the Russian Ruble, Brazilian Real, and a number of Asian currencies, have lost the trust of the public in their function as a store of value.

Two (probably parallel) routes are likely to lead to improvements in the value storage function of private digital money: First, it is technically feasible to equip digital money with interest payments. Cash would be interest bearing for the first time in the history of money. Second, privately offered money could create higher value stability, in the form of a lower inflation rate, than legal tender.

It should also be noted that, over the last two years, many currencies, such as the Russian Ruble, Brazilian Real, and a number of Asian currencies, have lost the trust of the public in their function as a store of value. This lack of confidence in government money has led to the formation of local private currencies in some regions of Russia. In situations like this, the market potential of an inflation-protected method of payment becomes even more obvious.

If the fixed exchange relation between private and state currencies is eliminated, (variable) exchange rates will coordinate supply and demand of the private currency.

A key element in the design of private currency is the retraction of a fixed rate for redemption into government currency. To attain trust in and demand for the private money, the issuer must offer some promise for redemption in return.

E-gold

Gold & Silver Reserve, Inc. (G&SR)[12] issued an electronic currency called "e-gold" and backed it with physical gold (against which e-gold is redeemable at any time). The company's motivation was the desire to create a pure payments system, one vastly superior (in terms of stability) to the existing monetary system with fractional reserve requirements.

E-gold attempts to improve the function of money as a store of value by tying it to the stable value of gold. Moreover, its function as a means of payment is designed to perform better than other payment systems, particularly credit cards.

G&SR's main objection to the "fractional reserve system" lies in the dual function of banks as the administrators of the payment system on one hand, and financial intermediaries – by accepting deposits (*i.e.*, borrowing money) and creating fractionally reserved financial assets (loans) – on the other hand. The creation of money and credit lie in the hands of the banks.

According to G&SR, a less than 100 percent backing (fractional reserve) of the issued claims, a feature of financial intermediation, inevitably leads to destabilization of the payment system, as the redemption of the issued claims is systematically at risk. Furthermore, the danger of a bank going bankrupt, *e.g.*, due to heavy loss-making lending practices, is seen as an unacceptable threat to the payment system. The necessity to separate financial intermediation and maintenance of a payments system is derived from these fears. G&SR confines itself to the design and maintenance of the payments system. Within this system, financial intermediation is practiced by any entity other than the operator of the payment system.

The liquidity of the system is guaranteed by a 100 percent backing of e-gold with physical gold. The system is financed by various fees on transactions involving e-gold.

All users must hold an account at G&SR, where their portfolio of electronic precious metals (namely e-gold, e-silver, e-platinum, and e-palladium, or "e-metals"), is recorded in weight measures. The account must initially be opened with at least one of the precious metals (InExchange). This is done either by a transfer of e-metal from another account, deposits of precious metals or purchase against state currency at an exchange rate set by G&SR. E-metal is credited to a customer's account according to the deposit of the precious metal. Physically, the precious metals are stored in bank safes in the United States and Switzerland. The e-metal can now be used either for payments (spend), for an order of delivery of the metal itself (redeem), for exchange against other e-metals (metal-to-metal-exchange) or government money (OutExchange). Payment is initiated over the Internet. The payee transfers a certain amount (expressed either in the corresponding value of a government currency or in the weight of a precious metal) from his or her account to the payee's account. Physically, the precious metal remains deposited at G&SR.

The job of G&SR is to make the e-metal redeemable against the corresponding precious metal. This means managing a 100 percent backing of all e-metal issued. The character of the precious metals as stores of value is cloned on e-gold. A means of payment is simultaneously created, which – in contrast to gold itself – is divisible into smaller units, homogeneous with regard to pureness, easy and safely transferable and securely storable.

While banks subsidize the administrative costs of the payment system from the revenues of the financial intermediation, the costs of the e-metal system are disclosed in the form of fees and passed on to the user.

The charge for the customer consists of a bid-ask-spread at exchanges between e-metal and government currency as well as fees for storage, transfer and exchange of e-metal (payable in e-metal).

The fees for e-metal payment do not exceed the corresponding e-metal value of 50 US-cents, and the transaction is carried out within seconds with very low online costs. The credited e-metal is instantaneously available for further transactions. E-metal seems to be superior to some other payment systems such as credit cards or checks, in terms of its quality as a means of payment for transactions over the Internet.

Even though e-metal has the character of an electronic payment system and is designed for payments via the Internet, it differs greatly from the previously described forms of "digital cash." E-metal is an electronically saved claim for redemption against a precious metal. However, because it is not a digital owner claim, which is negotiable between parties without a clearing over G&SR's books, it is not appropriate to characterize it as "digital cash." It is realistic to speculate that G&SR's core business would include this. Together with the encryption technology of DigiCash, a digital token could be created that represents a negotiable owner claim of redemption against a precious metal, but is not bound to a person or an account: DigiGold [13] Storage on smart cards, similar to the technology used by Mondex, is also conceivable. Instead of using different government currencies, DigiGold, DigiSilver, DigiPlatinum and DigiPalladium could be stored on Mondex cards. They could even be used for the dull routine payments of everyday life.

Barter Systems

The lower transaction costs achieved by the use of the Internet could not only promote a renaissance of the gold standard, but could also reinvigorate the concept of barter exchange. We now discuss how these technological advances are likely to impact the extinction of our present monetary system or the

creation of a new financial system. The so-called local exchange trading systems (LETS) are closed exchange systems with a private currency that serves as the unit of account.[14] The system's participants have accounts valued in this distinct currency, in which all goods and services rendered or received are tracked. Positive or negative account balances are derived from discrepancies between the offer of a good or service and an appropriate compensation. To date, most of these exchange systems remain confined to "local" systems, due to the costs associated with transferring goods. One example is the Bartercard Trading Program, which claims to be the world's largest trade exchange by volume of trade turnover. Acting as a third party record keeper, Bartercard uses credit units called "Trade Dollars" to monitor the value of transactions. Bartercard members are issued with a plastic card and trade among them in a sophisticated fully computerized barter system. Authorization is conducted over telephone, but the Internet could be used for this purpose.

Money solves the two problems of barter: information (double coincidence of wants) and synchronization (double coincidence of timing of transactions). The use of money is founded on the principle of reducing the transaction costs associated with exchange. To put it in other terms: The use of money only makes sense when the exchange of goods is connected to transaction costs. Network computers and especially the Internet reduce the costs of searching for and transferring goods and services, especially for digitized goods like software, music, or consulting services. In this respect the growth of exchange clubs is conceivable and with the use of the Internet for the "wire over" of the goods the LETS are no longer locally confined. The Internet functions as a kind of stock exchange, coordinating supply and demand and executing the exchange of digital goods at very low costs.

A moneyless society based on barter exchanges will only develop in the unlikely event that the use of computers completely eliminates the transaction costs associated with exchange transactions.

Finally, the question raised at the beginning of this article can be answered. If digital cash continues to be tied to governmental money, cash will only evolve from paper to digits. Once the public has confidence in digital cash (no time soon), these techniques could become a vehicle for a revolution in the use of money.

Notes:

1. Hicks, J., *"Critical Essays in Monetary Theory,"* Oxford 1967, p. 1.

2. For advantages and disadvantages of stored value cards see Effross, W. "Consumer and Stored Value Cards: An Unhappy Marriage of Convenience?," *E-Money*, Vol. 1, No. 1, 1998

3. Overview at Fancher, C. *"In Your Pocket: Smartcards," IEEE*, February 1997, pp. 47-53.

4. Mondex homepage at *www.mondex.com*

5. For further details on the features and implications of the Mondex system see Stalder, F. and Clement, F., *"Exploring Policy Issues of Electronic Cash: The Mondex Case"* at *<www.fis.utoronto.ca/research/iprp/dipcii/workpap8.htm>*.

6. See Weaver, C. "Smartcards in the United States: What is Holding up the Show?" *E-Money*, Vol. 1, No. 4.

7. Mondex on the Internet at *www.mondex.com.*

8. www.multos.com.

9. DigiCash homepage at *www.digicash.com.*

10. See Birch, D., "The European Purse Scene: A Snapshot View and some Predictions," *E-Money*, Vol. 1, No. 1, 1998.

11. White, L., "The Technology Revolution and Monetary Evolution," in: *James A. Dorn (ed.): The Future of Money in the Information Age*, Washington DC, 1997, p. 18.

12. See their Homepage at *<www.e-gold.com>* for the following description of the system.

13. G&SR already trademarked this name.

14. For a further characterization of LETS refer to *<www.transaction.net/money/lets/>*.

Insurance Companies Lag in Web Stakes

Just 37 percent of insurance companies consider the Internet integral to their business strategy, according to a report by Booz-Allen & Hamilton. This compares to 16 percent of insurance companies in 1997 and just 11 percent in 1996.

The focus remains strongly on the Web as an additional marketing tool rather than as new means by which to sell insurance, according to the report.

The study found that over 50 percent of insurance companies invest less than USD500,000 per annum in Web development. Further, 60 percent of companies do not expect to sell insurance online within the next two years. The majority, 58 percent,were not in a position to respond to a basic email question from a consumer.

The findings are based on a survey of 45 insurance companies, from a mailing to 150 companies, as well as a review of 200 insurance Web sites, including the 150 companies surveyed.

For more information, visit *<www.nua.ie/euathinking.html>*.