

# Electronic Money

## As A Competitive Advantage

Ken Griffin, (E-mail: keng@mail.uca.edu), University of Central Arkansas  
Phillip Balsmeier, (E-mail: mnmk-pwb@nich-nsunet.nich.edu), Nicholls State University  
Bobi Doncevski, (E-mail: mnmk-pwb@nich-nsunet.nich.edu), Nicholls State University

### Abstract

*The use of electronic commerce is increasing rapidly and with it the use of electronic or digital money. A variety of options are available as to the form of digital cash one uses. Along with the increase in electronic commerce comes electronic fraud. Until secure electronic transactions are guaranteed, users should be cautious of giving financial information over the Internet.*

### Introduction

**D**igital money is the ultimate--and inevitable--medium of exchange for an increasingly wired world. With E-cash, you'll no longer need to carry a wad of bills in your pocket or fumble for exact change. Instead, you might carry a credit-card-size piece of plastic with an embedded microchip that you will "load" up with E-money you buy with traditional currency. Or, you might store your digital coins and dollars--downloaded over phone lines from your bank or other issuer of E-money--on your PC or in an electronic "wallet," a palm-size device used to store and transmit E-money.

This digital money will let you shop online, zapping money to a merchant over the Internet, or perhaps paying for a movie on demand over an interactive-TV network. It also has the potential to replace cash and checks for everyday purchases--in stores, restaurants, or taxis that accept E-cash. Businesses could also keep a stash of E-cash on hand for buying office supplies, or use it to transact directly with each other instead of going through banks and electronic funds

---

*Readers with comments or questions are encouraged to contact the authors via e-mail.*

transfers.

But the advent of E-cash raises all sorts of questions, most of which remain unanswered: Who should be allowed to issue E-cash, and who will regulate those issuers? How will taxes be applied in cyberspace, which transcends physical boundaries? Who will set the standards? How do you ensure that payments made over the Net will be secure? How will consumers be protected? How will regulators police money laundering and counterfeiting on private networks?

### Definition of Electronic Money

The term electronic money is often used loosely to refer to a wide variety of proposed retail payment mechanisms. E-money products are defined here as "stored-value" or "prepaid" products in which a record of the funds or "value" available to a consumer is stored on an electronic device in the consumer's possession. The electronic value is purchased by the consumer (for example, in the way that other prepaid instruments such as travelers' cheques might be purchased) and is reduced whenever the consumer uses the device to make purchases. In

contrast to the many existing single-purpose prepaid card schemes (such as those offered by telephone companies), e-money products are intended to be used as a general, multipurpose means of payment. Moreover, the definition covers both prepaid cards (sometimes called "electronic purses") and prepaid software products that use computer networks such as the Internet (sometimes referred to as "digital cash"). From a policy point of view, the main interest in these schemes lies in who issues the prepaid value, how it is used as a means of payment and the impact on central banks' balance sheets.

E-money as just defined differs from so-called access products, which are products that allow consumers to use electronic means of communication to access otherwise conventional payment services (for example, use of a standard personal computer and a computer network such as the Internet to make a credit card payment or to transmit instructions to make funds transfers between bank accounts). The significant novel feature of these access schemes is the communication method (e.g. the use of a computer network rather than a visit to a bank branch) and so, although they are of interest, they do not raise the same concerns as e-money schemes and are not considered further in this report.

### **E-money and the Internet Phenomena**

It is predicted that most business and personal transactions will be performed by electronic means in as little as five years. The statistics are indicative to the present and future consumer and supplier demands. According to Mark Lottor's Domain Survey, from July 1993 to July 1995 the overall number of registered host computers connected to the Net rose from 3.2 million to 6.6 million. By the end of the decade 120 million computers will be connected to the Net, according to the Internet Society (Reston, VA), which bases its projection on Lottor's survey. These statistics are machine counts. The numbers of users are much higher, but can only be estimated. Most analyst's estimates of total Internet users range from 20 to 40 million people. Another 200 million people will

join the Internet worldwide by 1999, according to IDC.

The growth of businesses joining the Internet has also risen dramatically. Everyday, approximately 150 new businesses come onto the Net, and their numbers total about 40,000, according to Thom Stark, owner of Start Realities, a consulting firm in El Cerrito, CA. The Bureau of Business Research at American International College (Springfield, MA) surveyed executives at 48 Forbes 500 firms to find out their plans for marketing and selling on-line. Their combined sales were \$188 billion and 765,000 employees. The executives predicted that, on an average, 67 percent of the firms in their particular industry would have customer on-line access, and 37 percent of the firms annual sales would come from the Internet and on-line services.

A switch to e-money seems to be where computer software companies and businesses are directing most of their energy. E-money is money that trades hands along the Internet, for the most part outside the network of banks, also excluding checks and paper currency managed by central banks and the commercial banking system. The legal tender of tomorrow will need to have the characteristics compatible with the electronic network. Paper money will most assuredly not be the wave of the future, but cryptographically sealed digital dollars (e-money) stored on a microchip-loaded smart card or on the hard disk of your computer. Smart cards will be no larger than the wallet you carry in your pocket. If you consider how banks and financial institutions handle your money today you will realize that digital money has been around for quite some time. Most business is conducted from computer to computer, just digits in a field.

Computer links between businesses have already created an Electronic Commerce that has been slowly integrated into our everyday business transactions. Most individuals normally use credit cards, ATMs, automatic debit and credit transfers. Eliminating current currency for electronic money will not be too difficult for these and future computer generations. Even the com-

puter illiterate will be coached and encouraged to use digital cash by promotional schemes and user friendly applications.

AT&T is working with CFI to offer home banking through 90 banks and thrifts. DigiCash in Amsterdam is experimenting with its own money. NatWest in the U.K. offers the Mondex Smart Card. American Express, Citicorp, VISA, Sun, Microsoft, MCI and many others are investing heavily in E-Money alternatives. Computer scientists and business executives are working furiously to create safe software to handle this new innovation, before their competition does. They realize that change is inevitable, and the "electronic gold rush" is on a short timetable.

### **E-money Versus Credit Cards**

Credit-card-based systems have the advantage of seeming familiar to consumers. But the card systems don't do everything cash can: They're not anonymous, they do not work person-to-person, and they have credit limits. They're also not suited for the grassroots economy the Internet makes possible, where any outfit or individual can sell its wares, whether a newsletter or a stock tip. That's where E-cash comes in. But E-cash needs to be just as secure as credit cards for people to use it. David Chaum, CEO of pioneer DigiCash in Amsterdam, has done the most to solve this problem. He has devised a clever system that uses so-called public-key cryptography that, like encryption, makes it possible to send sensitive information over the Net. But Chaum's big breakthrough was "blinding" technology, which lets the issuing bank certify an electronic note without tracing whom it was issued to. The result: Your E-cash, unlike an encrypted credit-card transaction, is as anonymous as paper cash.

### **E-money Categories**

It cost money handlers in the U. S. approximately \$60 billion a year to process money transactions. E-money is a viable alternative to lower the money handler's costs incurred while

processing conventional money transactions. This won't happen all at once, and paper money will probably never become obsolete, but bills and coinage will increasingly be replaced by some sort of electronic equivalent. Checks fall in the same category; they are slow and costly to process. The first use of electronic money (e-cash) for real transactions on the Internet was announced in January, 1996, by Mark Twain Bank in St. Louis, MO. The bank started accepting applications for accounts that can be used to withdraw and deposit e-cash over the Net. Calling it "a beta test of e-cash using real money," Mark Twain Bank said it would limit the test to 10,000 accounts. E-cash is just one form of e-money. The following will explain how e-money will work in various forms.

### *E-cash*

Digital cash consists of a token that you can authenticate independently of the issuer. You can withdraw digital currency from an Internet bank account and store it on your computer's hard drive or on Smart Cards the size of credit cards. E-cash uses digital signatures, usually called coins, which represent a fixed value. The coins establish their own authenticity by a complex software algorithm or through tamper-proof hardware. DigiCash, a Dutch company, holds a patent for E-cash. Using e-cash is similar to using a bank's automated teller machine, but using your hard disk instead. When paying for something on the Net, you confirm the amount, purpose, and payee, and your e-cash software transfers the amount from your disk. Sellers deposit the e-cash they receive into their accounts.

### *Digital Checks*

A digital check uses a paper-check model. You can't validate digital checks without involving the issuer. You sign and endorse the checks using digital signatures. Digital certificates establish the payer's identity and bank information. Authentication is achieved using the public-key system. The payer digitally signs a form containing a description of the transaction,

payer and payee information, the amount, and a time stamp. The payee, who may receive the signed form by way of public e-mail or various other forms of electronic communication, can validate the check using a public key and deposit it to collect payment. Digital checks integrate with automatic ordering and billing systems. They also tie in well with existing interbank clearing houses.

### *Digital Bank Checks*

Guaranteed by a bank, these checks function similarly to digital cash, minus the anonymity. You use it when the payee requires a bank certificate that sufficient funds are available and will be paid out. Users buy the checks from a bank, which redeems each serial number only once. Digital bearer bonds with interest coupons are a special type of a digital check. The bearer periodically sends in a coupon to the issuer to collect interest at a specified rate.

### *Smart Cards*

Smart Cards usually use a debit system: The prepaid card stores value that the holder can spend. Merchants receive payments through the card organization. Particularly in Europe, old-style Smart Cards -- simple memory cards that are not too smart- are popular for pay phones, vending machines, road tolls, photocopiers, and other pedestrian uses. Some companies are introducing new, more sophisticated cards that contain embedded micro-processors. The cards are much more tamper-resistant than their predecessors. In some implementations, users combine the cards with electronic wallets that can read the data on the card and exchange value with other users.

Arkansas Systems, one of the largest vendors of Automatic Teller Machine software in the world, states that security is the key to growth of electronic banking for individual consumers and businesses. Arksys has just released a state of the art security system that can eliminate security concerns almost entirely. It is designed for use on the Internet and Intranets and is

called Safe-ACCESS. It uses a smart card to send information to a laptop or desktop computer via a smart card reader or a special diskette. The smart card is inserted into the special floppy first and then the diskette is inserted into the normal floppy drive. With the smart card and Safe-ACCESS, the user has three levels of security to protect a transaction. Until now, all that was needed was a password, which might be obtained by an unauthorized user. With the smart card you still have the password but you also must physically have the card. If the card is stolen it can be invalidated. The system also operates with something called a certificate, which electronically authenticates the identity of people and businesses. These certificates are issued by businesses called certificate authorities. Before a company is issued a certificate the certificate authority determines if it is legitimate. These certificates are downloaded from the certificate authorities to the smart card where they become digital signatures. To access their accounts, users will insert their smart cards in the reader or special diskette and bring up their browser, usually Netscape or MicroSoft Explorer. They then go to the banks' Internet site where their certificates and passwords will be verified. Once verified, the user can conduct a variety of transactions with the bank. Businesses and individuals can transfer funds, order checks, get current interest rates, open new accounts, stop payments on checks, and even order rolls of coins to be delivered.

### *Electronic Coupons and Tokens*

Electronic coupons, the electronic equivalent of the supermarket coupon, are functionally similar to cashier's checks, but they can be redeemed only at the issuing organization. They usually pay for some specified service and can't be redeemed for cash.

Because so many different types of individuals, from home shoppers to corporate purchasing agents, will be spending e-money, digital currency will come in many formats. Netscape introduced Live-Payment, a system that enables companies to accept encrypted credit card pay-

ments from customers for products sold on their Web sites. Netscape also announced that future versions of Navigator would include electronic wallet technology that will organize user's credit card payment information and maintain an electronic ledger of receipts and transactions. "Electronic purse" is being designed by Visa, who is collaborating with financial institutions, to be used for low cost items at convenience stores, grocery stores, gas stations, pay phones, video games, and vending machines. At Mankato State University in Mankato, Minnesota, students are issued "MavCards," to be used for MCI long-distance calls, dining-hall meals and cash services like laundry, photocopying, and vending machines. Of course lets not forget the giant Microsoft who has bought \$1.5 billion worth of stock in Intuit, Inc. a financial software company that was moving towards automating money.

With all the development and merging within the computer industry, and with electronic money as one of their top priorities, it would seem to demand that the governments of the world get together and implement a scheme to make the shift of a new money system in an orderly fashion. But that's not happening. The U. S., according to sources, seem to be "clueless." When Steven Levy, author of *E-Money (That's What I Want)*, contacted a spokesperson for the Federal Reserve to ask about electronic cash he laughed at him. He states, "It was as if I were inquiring about exchange rates with UFOs. I insisted he look into it, and he finally called me several days later with the official word: the Federal Reserve is doing nothing in that area." However, it seems the right hand does not know what the left is doing. The federal government has been making long range plans for some time now. They are not necessarily concerned *with what* is being spent as much as they are concerned with *how much* is being spent *by whom*.

The mid-1980's IRS Secret Five Year Plan foresaw a computerized dossier on every citizen, logging permanently even the most minute financial transactions. Financial freedom could be at risk with the development of e-money, and the decisions made now will deter-

mine how much of our privacy we will lose. Individuals questioned about privacy and the IRS were not afraid of the agency knowing what they spend as much as they didn't particularly care for the idea of a watch dog tracking them 24 hours a day. If electronic money is not secured from prying eyes, the IRS, along with every marketing firm in the country, will know the most intimate details about you and your family. The credit card sniffers are waiting in the wings also to snatch every unsecured credit card that passes their way. There are several electronic security programs in the development stage. David Chaum, founder of DigiCash, Amsterdam, Netherlands, has made it his main objective to develop anonymous digital money. He has devoted most of his energy to developing cryptographic technology. Cryptograph is a digital code that secures information as it travels on the Internet and protects you from those who are inclined to snoop or steal. Firewalls are being used to stop system intruders before they can enter your network. Pretty Good Privacy is a high-security cryptographic software application, distributed by MIT. The security problem is being addressed in every possible way by several companies. When it is resolved the net will explode into a mega market of businesses and services, open for business 24 hours a day.

### Global E-money

Western Europe showed the second largest amount of Internet growth with 1.4 million hosts in July 1995 compared with 730,000 hosts in July 1994. However, on-line networking will be very slow due to the lack of proper service and the exorbitant prices they must pay to get on the Internet. The European citizens want to participate in all the Internet has to offer, but their telephone companies want to fix the price of access and their governments want to set the rules.

Where Europe is really taking center stage - and the world is watching - is through their implementation of a new monetary system. They will change to one currency called Euro. If they want to pay a bill, they don't send a check. They send a payment request and the relevant

account numbers to the bank, which transfers money from the customer's account to the merchant's. Their electronic commerce will continue to evolve, but like North America they will feel pressure to accelerate their pace.

Much of Europe's research on e-money focuses on Smart Cards. Conditional Access for Europe (CAFE), a project in the European Community's ESPRIT research program, is developing a secure electronic payment system based on Smart Cards and several types of electronic wallets with infrared transceivers. You can run the protocols using standard PDAs. Thirteen partners from several countries, including the Netherlands, Denmark, Britain, France, and Germany are involved.

In Austria, 2.5 million consumers already carry a card that has the standard ATM magnetic stripe as well as the embedded Smart-Card chip. In the British town of Swindon, Mondex Smart Card, developed by British Telecom and two major British banks, National Westminster and Midland, stores the local equivalent of about \$250. These are currently being used for low cost items. Parents even have used them for their children's allowances. In Denmark, Danmont has distributed over 100,000 cards with money for spending on such things as parking meters and laundromats. Similar systems exist in Portugal and Singapore.

The Netherlands on the other hand has one of the highest computer-per-head counts in the world. The first nation on the continent to privatize its national phone company, the Netherlands has a more flexible telecommunications infrastructure than most other European countries. Holland is highly visible in the European cybersphere.

Denmark, Finland, Norway, and Sweden are very progressive in the development of on-line technology. The most recent statistics show them in the top 20 countries in number of computers connected to the Internet. They are a step ahead of many other countries because they have some of the world's best phone systems. They

also have governments who are open to new technology. The Danish government has published a proposal (Information Society by the Year 2000) that envisions all citizens having an electronic citizen's card with picture and PIN code taking the place of identification papers, marriage certificate, health insurance card, driver's license, etc. By the year 2000, all public authorities are supposed to have an e-mail box to which all citizens and companies can send letters and information. The Danish government and its citizens are calling for universal access to the Internet and an educational system that teaches all people to master it.

### **Potential E-money Limitations and Unanswered Questions**

Who is going to create the monetary value? In other words, who will back up the money, assuring trust. Will it be government? Banks? Visa? The New York City Transit Authority?

The problem has not been solved yet although needs immediate attention. Some think this issue only poses a great threat to the banking system of a nation. Yet others seem to think that, if universally trusted, a digital currency system can, in effect, float on its own momentum. "If you have money on the network, you can make private money on the network," says Eric Hughes, a co-founder of the privacy champions, the Cypherpunks. He is now exploring the possibility of setting up a cyberspace bank. "It's easiest not to turn the money into paper if you don't have to."

What security features will be included? How will these systems protect against fraud? Can they be hacked or counterfeited? What will be the trade-offs between ease-of-use and security?

Smart cards have to be tamper-proof so people can't reverse engineer them and double-spend. The prime protection is cryptography. "The bits in a container have to move from one to the other," explains Scholom Rosen of Citi-

bank. "When you're done, you have to have less in one container and more in the other. Also, your transaction can't be intercepted. Crypto can secure the transition. How strong the crypto is depends on who's going to try to break in - if it's the Mafia or a national government, they'll have plenty of resources." The most immediate concern of anyone attempting to produce a digital form of currency is copying. As anyone who has copied a program from a disk to a hard drive knows, it is totally trivial to produce an exact duplicate of anything in the digital medium. What's to stop me from taking my one Digi-Buck and making a million, or a billion, copies? If I can do this, my laptop, and every other computer, becomes a mint, and infinite hyperinflation makes this form of currency worthless.

The answer to the problem of digital duplication lies in using digital signatures to verify the authenticity of bills. Only one serial number would be assigned to a given "bill" - the number itself would be the bill - and when the unique number was presented to a merchant or a bank, it could be scanned to see if the virtual bill was authentic and had not been previously spent. This would be fairly easy to do if every electronic unit of currency was traced through the system at every point - but that would bring about exactly the kind of surveillance nightmare that gives Chaum the chills. How could you do this and unconditionally protect one's anonymity? It is a question still not answered.

Another question unanswered is: will e-money cards work so the value will be restored if they're lost? Everybody seems to agree that smart cards holding digital cash should provide an option to punch in a Personal Identification Number before buying something; but there is also a consensus that most people won't use that option. "The consumer won't bother with that," says Visa's Michael Nash. "The key here is that we imagine this as expanding what you do with credit cards. We do not think the electronic purse is appropriate for people buying jewelry or automobiles." In many systems - Mondex is a good example - losing your stored-value smart card is like losing a wad of bills. Don't carry

more than you can afford to lose.

Potential conflicts may evolve over who's going to regulate electronic money? At the moment, all the players are proceeding as if no one is. They extrapolate a regulatory system growing out of the current one, while they are aware that as the digital economy becomes pervasive there may be calls for new limits and regulation. As for now, the rush is to get everything in place, and no traffic cops seem to be slowing anybody down.

The continued expansion of the Internet in foreign countries will be closely followed by developments of more and more e-commerce inside and outside their countries. However, differences between national data protection laws have resulted in obstacles to transfers of personal data. This has been a particular problem, for example, for multinational companies wishing to transfer data concerning their employees between their operations. Such obstacles to data transfers could seriously impede the future growth of EDI (Electronic Data Interchange) and e-commerce internationally. Cryptographic software is restricted for export in many countries. Australia requires written permission to exporting cryptographic equipment designed to ensure the secrecy of communications or stored information. COCOM (Coordinating Committee For Multilateral Export Controls) is an international organization consisted of Japan, Australia, and all NATO members which has decided to allow export of mass-market cryptographic software. Some member countries of COCOM follow its regulations, but others, such as Germany and the United States, maintain separate regulations.


### **Conclusion**

With the passing of each day a new development or invention is announced. Standardized e-money, legal Internet guide lines, a national standardized security protocol, and a globally interactive e-commerce will be developed and announced which will change the world forever.

When will some entrepreneur seize the opportunity to supply the entire world with a new and better money to replace rapidly evaporating national currencies? Suppose he piles up gold and silver somewhere, and issues credit E-money against that pile? Suddenly national currencies have to compete with a currency whose value does not depreciate daily, stealing from them minute by minute. National legal tender laws can no longer force free-wheeling "Netizens" to accept national fiat currencies, and they have every reason of self-interest to use gold and silver backed E-money. Soon this gold-backed E-money would crowd out its competition. On the Net transactions in national currencies would become a thing of the past. The Net people will quickly transfer the habit of using good money to their daily lives. If they don't have to live with depreciating national currencies in virtual reality, why suffer with them in real life? Within 5 years or less, specie-backed E-money could completely replace national currencies and revolutionize the world economy. Government economic controls and inflation would become threats of the past.

It will be interesting to see what the Twenty-First Century brings us: e-money confusion or increased convenience. Change is inevitable once people are convinced the Internet is a safe and secure place to do business. Businesses must be prepared once the consumers start transferring e-money by using the Internet in ever increasing volume.

### Implications For Future Research

Future research should focus on the safe, secure transfer of electronic cash transactions and the legal changes that will surely accompany the growth of electronic commerce and the use of electronic money. With the major players like VISA and MasterCard endorsing continued development of safe electronic transfers and the banking industry looking for alternatives that will replace traditional checks, expect more banking from personal computers at home. Also, electronic money will play an increasingly important role in the continued growth of global commerce. 

### References

1. Bournellis, Cynthia, "Internet 95," *Internet*, November 1995.
2. Dejesus, Edmund X., "How the Internet Will Replace Broadcasting," *BYTE*, February 1996.
3. Flohr, Udo, "Electronic Money;" *BYTE*, June, 1996.
4. Levy, Steven, "E-money (That's what I want)," *Wired*, Netscape, December 1996.
5. Loeb, Larry, "Internet News," *Internet*, January 1996.
6. Payne, Jeffrey and David Pool, "Forging Ahead," *Internet*, November 1995.
7. Reynolds, Alan, "E-Money and a Tax System for the Twenty-First Century," *Wired*, Netscape, December 1994.
8. Sanders, Franklin, "E-Money Paradise or Prison?" Swiss American Trading Corporation, Netscape, 1996.
9. Holland, Kelly and Amy Cortese, "The Future of Money," *Business Week*, 06 January 1995.
10. Yount, Sheila, "ARKSYS Banks On Its Smart Card", *Arkansas Democrat Gazette*, Dec. 29, 1997.