Digital Cash Payment Systems

Leah Fera
Mike Hu
Gene Cheung
Mark Soper

December 6, 1996

Abstract

The recent explosion in the popularity of the Internet has been accompanied by considerable interest in using this worldwide collection of interconnected computers as a medium for commerce. While electronic commerce in general is not itself a novel concept, the dizzying pace of change in the computer networking landscape of late promises to bring with it exciting new ways for individuals and companies to conduct business.

In this paper, we begin by presenting a broad overview of current electronic commerce technologies. We then focus on one particularly interesting form of electronic payment: digital cash. We define specifically what is meant by digital cash, what a digital cash system entails, how such a payment system compares to other existing and proposed payment systems, and discuss the challenges that must be addressed in implementing digital currency on a wide scale. We provide a detailed description of several emerging digital cash systems, and address the advantages and disadvantages that the proliferation of a such a system might entail.

1 Introduction

Today the term electronic commerce suggests to many the purchase of goods and services via some sort of on-line marketplace. In reality the term is much more broad, and is subject to a multitude of interpretations. One might argue that electronic commerce can be loosely applied to any method or system whereby two or more entities exchange funds, goods, services, or commercial information through the use of digital technology. So given this broad definition, it's quite a difficult task to give an example of a modern business process that doesn't involve electronic commerce in some way.

Equally challenging is the task of devising an accurate taxonomy to describe systematically the various forms of electronic commerce and the relationships between them. In general it is useful to consider three major classes of electronic commerce:

- **Electronic Fund Transfer Systems** - any electronic method for payment, or transferring money or funds from one entity to another. This class includes a wide variety of systems, including ATM networks, credit/debit cards, Electronic Fund Transfer (EFT), smart cards, digital currency, electronic checking, etc.

- **Electronic Commercial Information Transfer System** - any system through which two or more businesses exchange commercial information electronically. Examples include the system used by Federal Express and its customers to track package delivery, Electronic Data Interchange (EDI) [1], etc.

- **Electronic Marketplace** - any system through which buyers can browse and purchase goods or services electronically, and/or sellers can display and distribute goods or services electronically. Such on-line marketplaces have emerged on the World Wide Web, and one might also include cable television shopping networks in this class.

Most any particular electronic commerce system falls into one of the above classes, although certainly many systems may involve components from two or all of the above, and may also involve more traditional forms of interaction that wouldn't be considered electronic commerce. It should be evident that electronic commerce encompasses a very broad range of systems and technologies.

This paper focuses on one particularly interesting example of an electronic payment system, namely *digital currency*. We define specifically what is meant by digital currency, what a digital currency system entails, how such a payment system compares to other existing and proposed payment systems, and discuss the challenges that must be addressed in implementing digital currency on a wide scale. We provide a detailed description of several emerging digital currency systems, and address the advantages and disadvantages that the proliferation of a widespread digital currency system might entail. To understand digital currency it is useful to first consider electronic payment systems in general.

2 Overview of Electronic Funds Transfer Systems

As defined above, an electronic funds transfer system is any method through which payments are made or funds are transfered electronically. This category itself is quite broad, ranging from existing retail bank offerings such as the Automated Teller Machine (ATM) network, debit card accounts, credit card accounts, employer EFT arrangements, and on-line bill payment, to emerging concepts such as Internet fund transfer systems, digital currency, etc.

The goal of this paper is to address emerging payment systems that are based on an interconnected network of computers, such as the Internet. After considering how one might expect to accomplish a commercial transaction on the Internet, it is possible to group such systems into three categories: secure credit card presentation, credit-debit instruments, and digital currency.[10]

2.1 Secure Credit Card Presentation

One way to pay for goods or services over the Internet is by leveraging the existing and mature credit card system. For years consumers have made purchases over the telephone by supplying credit card account information. This model can be readily extended to the Internet. The primary advantages of this form of payment is the ubiquity of credit cards. Most consumers already have them, and most sellers already accept them. The primary disadvantage is that the Internet is not inherently secure, meaning that credit card numbers transmitted over the Internet can be intercepted and misused quite easily. Another potential disadvantage is that the overhead expenses incurred in credit card transaction processing prohibit small purchases on the order of a few cents.

Several implementations of this form of payment system have been proposed. Netscape's current web browser and server software have functionality built in to facilitate encrypted transmission of credit card information. Here the exchange between the merchant and the credit card entity, often referred to as the acquirer, is done via the traditional method, namely private telephone circuit. New systems are under development where the merchant-acquirer exchange is done via the Internet as well.

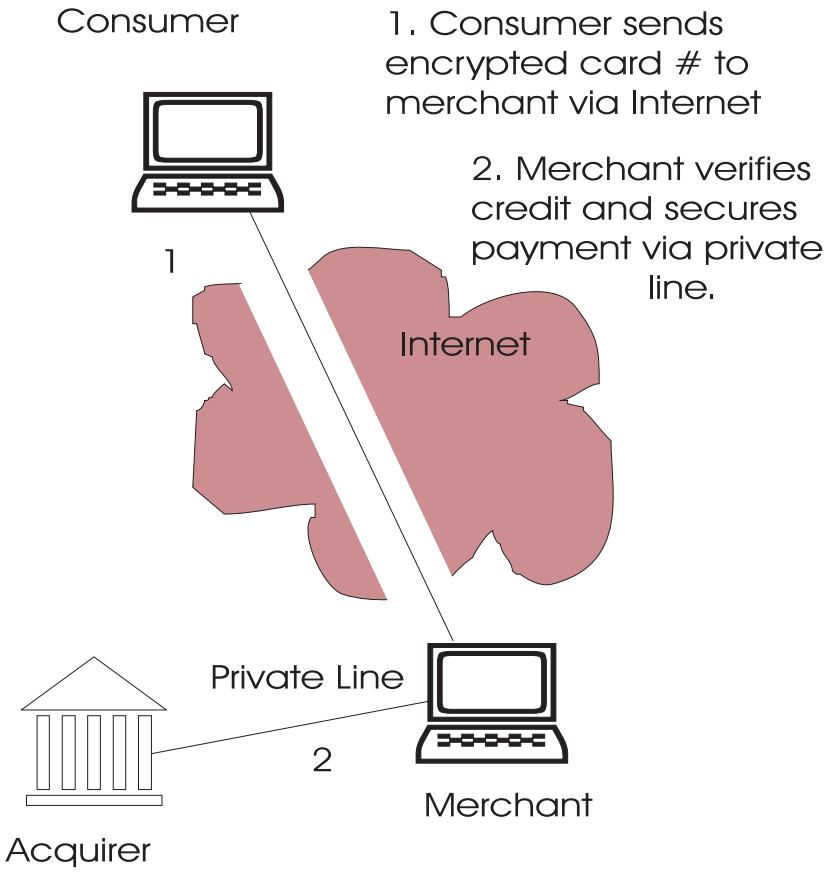

Figure 1: Secure Credit Card Presentation

2.2 Credit-Debit Instruments & Electronic Checking

Another way to accomplish payment on the Internet is for both the buyer and the seller to maintain an account with a third party payment server. The consumer must have a registered account, either credit or debit, with the payment server. The merchant must have an account with the payment server as well so that the seller's account can be credited when a purchase is made.

This form of payment method is essentially an on-line version of the existing credit card/debit card model of commerce, and it shares with these payment models one primary advantage: auditability. The payment server maintains a record of the transaction containing the identities of both buyer and seller and information about the nature of the transaction, the amount, etc. Digital credit/debit may hold several advantages over existing credit/debit and checking systems, including the reduction of paperwork costs, increased transaction clearing time, the elimination of bounced checks, and greater flexibility. [11]

Although such systems have been deployed on the Internet, including USC-ISI's NetCheque[10], CMU's NetBill[12], and First Virtual's Infocommerce[5], they have yet to gain popularity. Neuman and Medvinsky offer the following insight: *For credit-debit or electronic currency systems to move beyond trials with play money, a separate tie to the existing banking system is needed to convert account balances and electronic currency to and from real money in a customer or merchant's bank account.* [10] The primary differentiating factor for providers of this service will likely lie in the details of the cost and convenience of this reconciliation between on-line and real accounts.

The third way in which payment could be made over the Internet is via a digital currency system. Such a system would enable transactions almost identical to those that currently take place with normal paper currency, except that the bill or coin that represents value in the paper currency model is replaced by a digital certificate, essentially a string of bits.

The digital cash certificate can be written onto a card, or can be represented in purely electronic form. The overall digital currency system can be considered to be independent of the physical medium on which the digital cash is stored and transmitted.

The primary advantage of a digital cash system is anonymity, while the primary disadvantage is the issue of counterfeiting. Anonymity makes a digital cash system desirable for consumers who do not wish for merchants, governments, or other organizations to be able to monitor their transactions. However, ensuring that each currency certificate is not spent more than once may involve enormous database and record-keeping requirements.

Nascent digital currency systems are beginning to gain popularity on the Internet today. The remainder of the paper discusses examples of these systems, including DigiCash[?] and CyberCash[8], and addresses in more detail the issues surrounding digital currency in general.

3 Requirements of a Digital Cash System

The digital cash industry is in its infancy. In order for digital cash systems to become useful to Internet community, they must meet various requirements. Some of these requirements apply

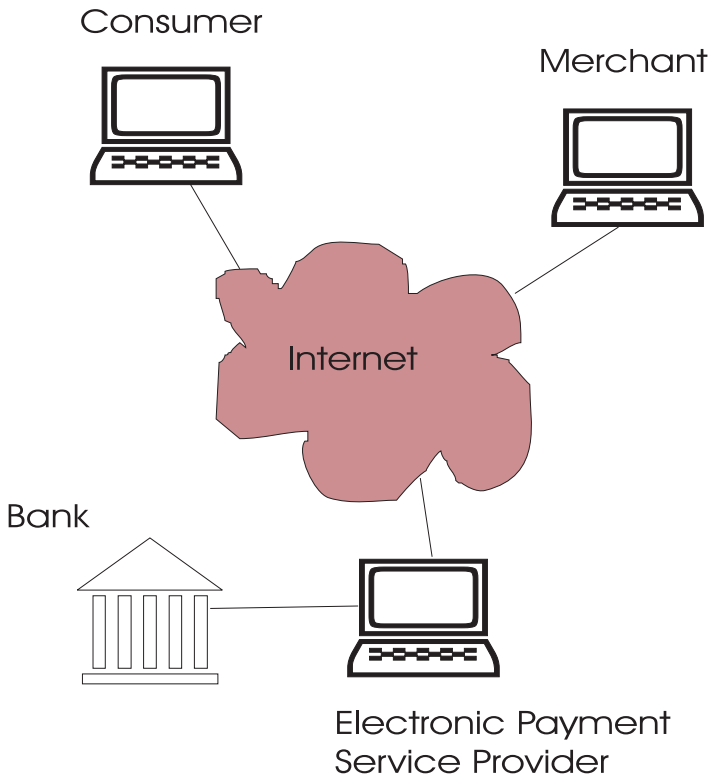

Figure 2: Electronic Credit-Debit/Checking Model

to any hard currency, while others are necessary due to the nature of the Internet. In this section we describe some of these requirements and contrast them with properties of currency.

3.1 Security

While security has always been an issue with the storage, transport, and exchange of hard currency, the issues involving digital cash are much different. Banks, for example, deal with the physical threat of robbery by investing resources to maintain large vaults, to hire security guards, and to hire armored trucks to transport currency. On-line cash transactions present an entirely different set of challenges. The threat of robbery is much more subtle. This threat comes in the form of malicious users who exploit weaknesses to attack the network itself and attempt to break into computer networks. Without effective security measures to protect digital cash, businesses and consumers will have no confidence in the system, and the risks involved with using such a system will outweigh the benefits. Therefore, the most sensitive issue among digital cash companies is the security of digital cash and cash transactions.

Security has always been an issue on the Internet because of the relative ease of others to perform covert activities over the network. It is well known that third parties have been able to easily eavesdrop, modify messages, and spoof messages. Eavesdropping on data en-route in the network can result in the theft of sensitive information such as account details and credit card numbers. By modifying messages in the network, the attacker can illegitimize the transaction by altering the payee or the amount of the transaction. Finally, spoofing is used

by attackers to masquerade as other parties. The attacker can fool the system or unsuspecting users into transferring money to himself. By performing these activities, malicious individuals can severely jeopardize the system. Therefore, digital cash systems must be impervious to these forms of attack. To prevent eavesdropping and message modification, the trend is to use cryptography to encrypt transaction messages such that only the intended recipient has the ability to decode and understand the message. As a deterrent to spoofing, digital signatures and certificates are used to authenticate the identities of the communicating parties.

In addition, digital cash systems must be foolproof to the electronic counterpart of counterfeiting. While counterfeiting paper money is a complex process that the average person is unable to perform, it is relatively easy for someone to duplicate digital cash either by merely copying data, or by reconstructing a data pattern. Thus, digital cash systems must be able to distinguish between bank-issued money and forged money. In addition, the system must be able to track digital cash such that the same money is not spent multiple times by a single or multiple users. A common method to perform these functions is to track all issued digital cash in a database. Whenever a transaction occurs, the cash is checked against the database to validate its legitimacy in both of the above senses. However, questions arise regarding the scalability and management of databases for such purposes. Whether the system tracks all digital cash that has ever been issued or only outstanding (unspent) cash, the database will grow with the increased usage of the system.

3.2 Anonymity

One characteristic of currency that sets it apart from other forms of payments is that cash transactions are anonymous and untraceable. When a cash transaction is made, the only record made is the amount of the transaction and that the transaction took place. In the case of hard currency transactions, this record comes in the form of a receipt. The identities of the parties are not divulged in any way and the receipt is untraceable to the parties. Thus, there is no risk of names being released or sold to solicitors, nor is there the risk that spending habits will be tracked by an organization or agency.

In the case of digital cash, it would be extremely easy for vendors to record and track consumers' spending habits since all transactions are done on-line. Thus, the prospect of an anonymous payment system is very attractive for consumers. Furthermore, the anonymity of such a system would not require other sensitive information to be transmitted across the network, such as credit card numbers, bank account numbers, and addresses.

Without the guarantee of anonymity, digital cash systems lose an important characteristic that distinguishes it from other forms of on-line payment.

3.3 Economies of Scale and Scalability

For digital cash to be successful, it must be widely accepted such that the economies of scale benefit consumers as well as businesses. With currency this isn't an issue. Since the government backs the currency and people have confidence in the government, all individuals and businesses in the United States accept currency as a valid form of payment. To illustrate

the importance of economies of scale, we will use credit cards as an example. Visa and Mastercard credit cards have become widely accepted by both consumers and vendors such that the benefit to both is great. One could argue that the Diners' Club Card is much less useful since it isn't as widely accepted by businesses, nor as used by as many consumers.

The economies of scale are affected by both consumers and businesses. Consumers must be assured that the purchase or acquisition of digital cash will be useful in purchasing a wide variety of products and services from a wide choice of vendors. Otherwise, the consumer will turn to other means of payment and the system will be undermined. Likewise, businesses must benefit by accepting digital cash as a form of payment, which comes in the form of an increased customer base. Without this additional benefit, businesses will have no incentive for adopting digital cash as a payment method.

Since the Internet spans the entire globe, a digital cash system that is accepted across the entire Internet would be extremely useful in increasing the economies of scale. However, issues involving transactions across international boundaries presents interesting challenges. For example, what would be the process of exchanging money of different currencies? How would international trade agreements be affected by the anonymity and ease of digital cash transactions?

Scalability is important in light of the growth of the Internet. Performance should not be affected by expanding the digital cash system nor by an increased rate of transactions. For integration purposes, an application protocol interface should be developed such that the system can be easily integrated into different applications. This would increase the potential for uses of digital cash. Furthermore, the system should support transactions that occur across heterogeneous platforms. A transaction should not fail because the involved parties use different computer architectures, operating systems, or computer networks.

3.4 Reliability

Reliability is another issue that exhibits a contrast between currency and digital cash. With hard currency, the only issue in reliability is the durability of the paper used to produce paper money. However, once a type of paper is designed or chosen, this issue does not persist. With a digital cash system; however, reliability presents itself in a different form. It must be reliable so that there is no risk of losing cash to failures in the network, software, or hardware.

The system must be robust to failures in a network so that there is no risk of losing digital cash during a transaction. Whether messages are lost during transmission or packet errors occur, the system should be able to recover the digital cash in the case of an interrupted transaction.

To guard against software and hardware failures, the system should allow consumers and businesses some method to guard against lost money from the loss of data. One method would be to allow customer and businesses to make backups of their accounts and allow backup accounts to be used in transactions if the original is corrupted by software or hardware failures.

3.5 Ease of Use and Flexibility

Just as currency provides an easy method of payment, an digital cash transaction must be simple to execute. The process of a cash transaction should be transparent to users. Once payments have been authorized by the user, the payment should occur without interruption to the user. Also, the digital cash system must allow users to easily divide their digital cash. Customers should always have "exact change" as long as the amount of digital cash that they have in possession exceeds the price of the product or service.

The system should allow portability such that users are enabled to spend their cash from any location in the network.

In addition to consumer-business transactions, peer-to-peer transactions should be supported. Unlike credit card systems and debit systems, individuals should not be excluded from the means to collect payments. This would allow the individual to sell services and items over the Internet and increase the usefulness of digital cash.

3.6 Summary

Integration of these ideas presents a challenging problem. We have shown that electronic money presents issues that are more complex that of currency in almost all facets.

One example of the complexity involved is the tracking of digital cash. The system must be able to track issued digital cash. However, the user may divide the cash into multiple portions that are spent at different times and places. Such tracking is not necessary with hard currency.

Furthermore, many of these issues have not fully been resolved. Proposed systems such as Ecash, CyberCash, and NetCash attempt to address these issues.

4 Monetary and Legal Implications of Digital Cash

The monetary and legal implications of digital cash should not be ignored. These issues involve digital cash itself as well as the legality of systems under certain scenarios. Although we will not discuss these in much depth, we will still bring to light some of these issues.

4.1 Monetary Implications

One can only guess the eventual effects of digital cash on the economy, although there are logical clues on which one can draw reasonable conclusions. With the perceivable ease and convenience of internet spending with digital cash, one would expect an increase in transaction velocity, similar to the effects due to the introduction of credit cards. The net effects of the increase in transaction velocity are: a) an increase in the price level of goods and services, b) an increase in economic growth.

The abstraction of digital cash may invite the public to create illusions of its value; the monetary mapping of a lump of gold to paper money is probably easier than the mapping from

a piece of paper to bouncing electrons in your virtual wallets. As a result, the introduction of digital cash to the public may force people to reexamine their conceptions of money, cash and monetary value.

Interest rates, which are traditionally believed to be related to the money supply, may also be affected. These are only several foreseeable effects on today's complex economy. Depending on the level of acceptance by the general public and the government's eventual regulations, these effects may play a important or non-significant role in our daily lives.

4.2 Who is Printing Digital Cash?

It is questionable whether digital cash is truly cash from an economic standpoint. If the cash is created by a financial institution, then its role is similar to physical cash: if a person deposits digital cash into his account, the financial institution is obligated to credit his account and acknowledge its monetary value. In fact, digital cash should be considered a type of currency in the calculation of money supply, not unlike other sources like physical cash and coins. For example, the calculation of money supply $M1$ is shown to be (panurach, 1996):

$$M1 = \frac{1 + (currency/deposits)}{LRR + (currency/deposits) + (reserves_{excess}/deposits)} * MB \qquad (1)$$

where $M1$ is the money supply, LRR is the legal reserve limit on bank lending, excess reserves are any nonobligatory reserves banks do not lend out, and MB is the monetary base. In the event that there is a large supply of digital cash, it will affect the currency to deposits ratio, thus affecting the total money supply of the economy.

On the other hand, if the digital cash is created by a non-financial institution, then it is really not cash in the economic sense; it is more like a coupon redeemable for goods at selected merchants. It is because the non-financial institutions serve as money exchange centers, where one unit of digital cash can be purchased or exchanged with one unit of physical cash. It has no effect on the money supply or the money creation process.

4.3 Legal Implications

The recognition of digital cash as a form of money by the U.S. government would open legal issues. The previous section provides sufficient criteria for and against recognition.

One such issue is taxation - should sales involving digital cash transactions be subject to sales taxes? One could argue on either side of this issue as described in the previous section. Suppose that digital cash transactions are taxable. This would cause severe administrative challenges. Since the decision on whether to levy sales tax is based on the physical locations of the consumer and vendor, the system would have to locate both parties without sacrificing anonymity. Given the current structure of the Internet, this is impossible even if the identity of the users are known. For example, consider users in the subdomain *cig.mot.com*. Users in this domain are co-located in Illinois and Texas. Furthermore, users may actually be physically located elsewhere, while using their accounts remotely in Illinois or Texas.

4.4 Foreign use of Encryption Technology

In the past, the U.S. government has limited the export of high-tech products and technologies because their use by other countries could provide national security risks. The implication of such an export restriction is that digital cash systems would be severely compromised because many of the encryption schemes proposed for use have been developed in the United States. It would be illegal for digital cash companies to distribute applications using such encryption methods to potential customers outside the U.S. This policy will have either one of two effects. First, if such encryption methods are used, foreign consumers and businesses would be excluded from the system, causing the economies of scale to be decreased. Alternatively, these encryption schemes would not be used in the system, and less effective methods would be adopted. This would undesirably compromise the security of digital cash transactions.

In the more recent past, the government has approved the export of an encryption scheme developed by CyberCash and another scheme developed by Hewlett-Packard, Microsoft, and Intel. However, it is unclear whether the government will require the possession of a recovery method to decode any and all messages encrypted with these schemes.

5 Proposed Digital Cash Payment Systems

We have presented some of the requirements and challenges for digital cash systems and will now describe some implementations that have been proposed. Although these systems are still in their infancy and the specific "requirements" for these systems are continually begin debated and modified, some fundamental issues remain.

Cash, my its nature, is an anonymous medium. Unlike checks or credit cards which use personal information to verify one's identity, it leaves no trace of the user. We can make purchases with cash without leaving a record. Therefore, cash is inherently untraceable and susceptible to illegal activity such as using stolen money to make purchases. On the other hand, cash does provide privacy to individuals who do not want big brother to become a reality. Developing an electronic cash system involves making decisions about the degree of security and the degree of privacy that will be ensured to individuals and organizations. The protocols chosen by e-cash developers are very important in creating a standard for electronic cash in the future.

5.1 The Ecash system by Digicash

Digicash, based in Amsterdam, is founded on the idea that anonymous electronic cash is a feasible and desirable electronic payment system. Their system provides the means for security using public key cryptography and anonymity using a patented technique called blind signatures. The founder of Digicash, David Chaum, claims that their system is mutually advantageous to organizations who desire increased accountability and to individuals who desire privacy in their transactions [7]. Other problems encountered with digital cash such as double spending and forgery are also addressed.

5.1.1 Ecash Fundamentals

Ecash is unique due to the design and implementation of a specific protocol used when making monetary transactions. Possible transactions include withdrawing and depositing ecash using a special bank account, paying a company for goods or services, and exchanging funds from person to person. The techniques that lie behind ecash are based in a software package which provides an easy to use graphical user interface in which the details of the protocol remain transparent to the user. The application can be run on several platforms. One can use a personal computer running ecash software under MAC OS, DOS, or UNIX, or a special "card computer" designed specifically to run the ecash protocols. If the computer is connected to the internet, payments can be made to anyone else who is connected since ecash coins can be sent anywhere that email can go. In addition, ecash can be transferred to cards that can be filled with ecash using an 'ATM' for ecash and spent at stores using special card readers [9].

Only a few banks, such as the Mark Twain Bank of Missouri, support special ecash "accounts", but if the ecash system becomes widely used, more will be established [11]. Both buyers and sellers must have a specific type of account at the bank. Buyers can transfer money from this account to the account's special Ecash Mint which acts as a buffer account. When a buyer withdraws ecash from the "bank", the funds come from the Mint. The ecash in the Mint is completely electronic and is no longer insured by the bank. Ecash units, also known as coins or notes, are identified by unique note numbers which are created by the user's computer at random when the user requests to withdraw money from the bank. The bank maintains a database of note numbers that have already been spent to eliminate the chance of double spending or spending stolen notes. Old note numbers are removed from the database to prevent it from growing too large since each note number has a built in expiration date [7].

5.1.2 Public Key Cryptography

Most Digital cash payment systems use encryption techniques to secure electronic transmissions of electronic cash and other important data. Cryptography is the key to maintaining these secure transmissions. In 1976, mathematicians Whitfield Diffie and Martin Hellman developed the idea of Public Key Cryptography which is used to secure the transmission of important data [6]. This technique is now being implemented by several Digital Cash Systems including ecash.

In previous encryption systems, one party used a secret code to encrypt a message, and the other party had an inverse code to decode the message. The problem was agreeing on the encoder and decoder to be used between two parties without relying on physical contact. With Public Key Cryptography, there is a public key known to the world (or whomever you do business with) and a private key, known only to the individual. To ensure that a message is only able to be read by a specific person, one can encode a message with the public key of the intended recipient, and only that person can decode the message using the private key. In addition, one may encode a message with their own private key and allow anyone else to read it using his or her public key. This will guarantee that the message was sent by a specific person, and not someone else claiming to be the sender. These two scenarios are shown in figure 3.

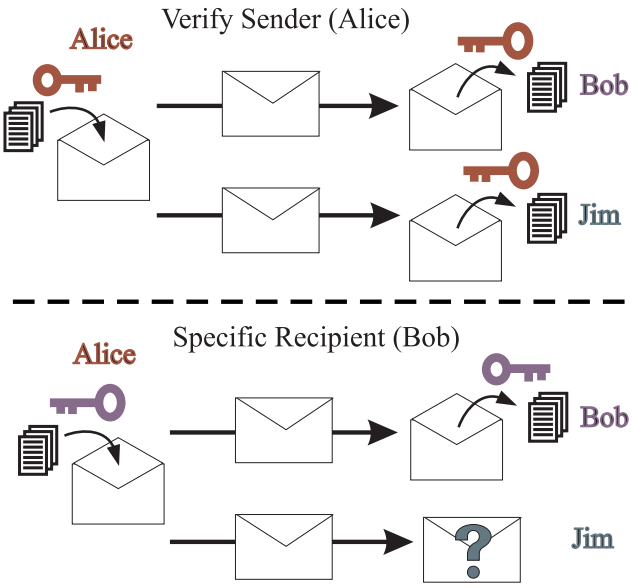

Figure 3: Two uses for Public Key Cryptography

Although public key cryptography can be broken in theory (by finding the correct private key), it is very unlikely. The encrypted data is only as secure as the private key. Therefore, the private key must be extremely difficult to discover. The techniques used today use a key that is on the order of 100 digits long that is the product of two very large prime numbers. The keys are so difficult to forge that it would require the fastest machines millions of years to do so. The odds of guessing a valid encrypted message are less than 1 in 10^{75}. [7] Digicash currently uses a key that is 768 bits long, but in the future, the ecash banks will decide on key formats and lengths for use with their customers [11].

5.1.3 Pseudonyms and Digital Signatures

In the ecash system, rather than using personal information to identify a consumer's account, an individual uses a different identifier with each account made with an organization. This identifier, or "digital pseudonym", is a public key that is known to the organization. The pseudonyms are created by a program on the user's computer. Although the details of creating the public key remain transparent, the individual has a say in the pseudonyms that are created and can assure that the same pseudonym is not used for more than one store. As a result, the information about a consumer cannot be easily linked to information from other stores since each has a different pseudonym corresponding to the same person. This gives greater privacy to the consumer.

The individual knows the private key (stored on his or her computer) corresponding to each pseudonym and uses it to "sign" messages containing ecash. The resulting encrypted message is called a *digital signature* because it can only be created using the individual's private key. Banks also use digital signatures to validate an ecash coin. Different digital signatures are used for different coin denominations. A coin with the bank's digital signature can be verified as genuine by an individual, store, or bank by applying the bank's digital pseudonym

to decode the signature. If the decoded message is appropriate (ie: fits the description of a coin), then the coin is valid.

By using digital pseudonyms and digital signatures, people and organizations, as well as coins from a bank, can be correctly identified (Their identity cannot be forged). However, using these techniques alone, a store can maintain information about a consumer since each transaction payment may be traced to the consumer via the note number known by the bank. This problem is solved using Digicash's concept of blind signatures.

5.1.4 Blind Signatures

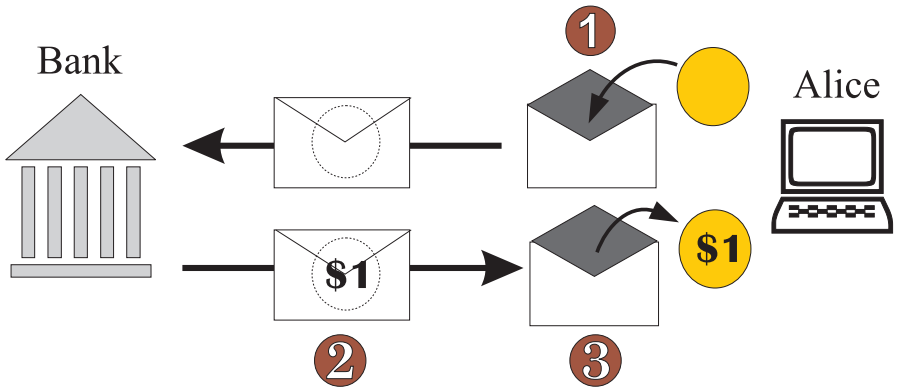

Figure 4: The envelope analogy for Blind Signatures

Blind signatures is a patented technique that allows payments to be unconditionally untraceable by preventing the bank from recognizing the source of a deposited coin. Blinding is a type of encryption that can only be removed by the party who created it. This is why the note numbers originate from the user's computer. The bank still adds a digital signature to legitimize the "blinded" note, and the user is able to unblind the note while keeping the digital signature intact. A useful analogy uses the idea of an envelope with carbon paper as shown in figure 4 . A note is created by a user's computer; it is put in a sealed envelope then sent to the bank. The bank cannot see what is inside the envelope (ie: the original note number), but embosses it with a stamp of its digital signature (specifying the denomination) so that the note gets validated through the envelope. The envelope can be removed by the user, leaving a valid note that the bank no longer recognizes as linked to the user. The actual implementation of the blinding process uses a large random number known only to the user to further encrypt the message so that the bank cannot learn the original note number. The blinding can later be removed by the user by applying an inverse process using the same random number. Blind signatures are the key to ecash's anonymity.

5.1.5 Payment Transactions

The following scenario describes the details of an ecash transaction between an individual, Alice, a shop that accepts ecash, and an ecash bank (Mint) and is diagramed in figure 5. It is

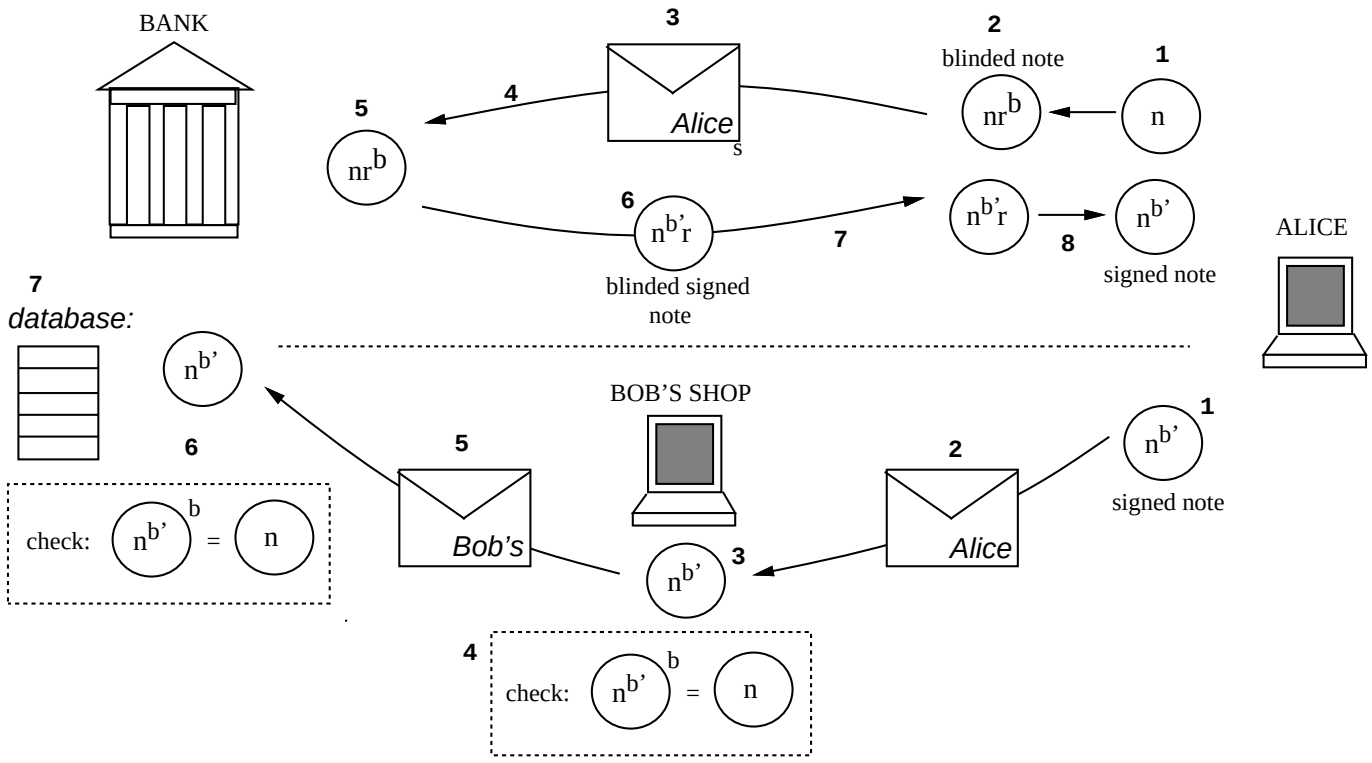

Figure 5: Withdrawing a note from the bank (above) and spending the note (below)

assumed that all necessary accounts have been set up. For simplicity, the transaction will be described with only one note. Rough details of the protocol are given. *Withdrawing a note from the bank*

1. Alice's computer creates a 100-digit note number, n, such that half of the number is created at random and the other half is a scrambled form of the first half. The resulting note number has a special repeated-halves property.

2. The note is "blinded" by combining it with another random number, r, and the bank's public key b, which represents the appropriate denomination. The resulting blinded note = nr^b.

3. Alice signs the message with her private key to verify her identity

4. The message is sent to the bank

5. The bank applies Alice's public key to strip off her signature from the message

6. The bank signs the note with its private key, b', representing the appropriate denomination corresponding to b. The exponent b' is applied to the blinded note to give $n^{b'}r$

7. The bank deducts funds from Alice's account, and the signed blinded note is sent back to Alice

8. Alice divides out the blinding factor, r, resulting in a signed note, $n^{b'}$ for her to spend

Spending the note

1. Alice agrees to purchase an item at a shop
2. Alice sends the signed note (now stored in her computer) to the shop after signing it with her private key
3. The shop strips off Alice's signature using her public key
4. The shop verifies the note is valid by applying the bank's public key to see if the result is a signed special note number with the repeated halves property
5. If the note is valid, the shop signs the note with its private key and forwards it ($n^{b'}$) to the bank
6. The bank strips off the shop's signature, then verifies the note's validity, just as the shop did, by applying the bank's public key, revealing the note number, n
7. The bank checks that n has not already been spent by checking its database
8. The bank adds funds corresponding to the note value to the shop's account

The note originally sent to the bank by the user (nr^b) cannot be linked to the note finally received by the bank, n. Even if the bank and the shop share all their information, as long as the blinding number, r, is not divulged by the user, the transaction cannot be traced to the user.

5.1.6 Solving Key Problems with Ecash

The key issues crucial to the success of electronic cash must be addressed by all implementations of e-cash in order to become a trusted, and widely used medium for monetary transactions. Digicash, using the mechanisms described above, has addressed each of the following issues.

- **Forging notes** This would involve forging the bank's signature which is equivalent to finding out the bank's private key. This is extremely unlikely using today's public key cryptography.
- **Stealing someone else's notes** Again, this would require finding out another person's private key.
- **Tracing an illegal payment** If a person's personal key was somehow used by an unauthorized party, the real user is able to release the secret blinding number so that the bank can trace the note to the criminal.

- **Accountability** A user cannot deny that he or she has made a transaction because the other party has received a message that is encoded with the private key known only to the sender (assuming the key was not stolen).

- **Double spending** A database of used note numbers at the bank can discover double spending. The cost of checking each transaction is actually less than for current payment systems [7]. However, checking a database will only detect the fraud after the fact since the transaction between the consumer and the shop has already been initiated. Other means of preventing double spending have been proposed which include observers, or special tamper-proof chips that monitor the transactions of the computer used by an individual or corporation.

- **Anonymity** The blind signature technique prevents organizations from tracing the notes involved in a transaction back to the user.

- **Restorability** If a user's computer crashes or the money is lost, a user can recover the notes by using a special recovery key along with the Mint's records from their transaction log. If the user is in the process of a transaction, the recovery those funds is only possible if the shop has not yet deposited the payment.

5.1.7 The Status of Ecash

Ecash was used in a trial program in 1994 with 30,000 customers and over 100 shops who agreed to accept ecash in exchange for goods and services [14] However, the ecash, known as Cyberbucks was and is not exchangeable for actual money. Stores are able to become ecash vendors by obtaining software from Digicash. In the future, many more customers and stores may join the ecash system. issues of One critic of ecash pointed out that the blind signatures concept has yet to be implemented in an significant system and that the patent by Digicash presents a barrier to the development of other electronic cash systems that wish to have an anonymous payment system [2]. Once this and other technical issues are solved, the medium of electronic cash faces other social, economic, and political challenges such as wide acceptance and consumer use, backing up the e-money, and regulation.

5.2 CyberCash

CyberCash Inc, a late comer in the Internet payment service provider market, is ready to compete with pioneers in the business such as Digicash. Based in Reston, Virginia, the company already has more than 30 web host companies across the country and is expecting more than 100 by the year's end. The keys to its success are: a) simple yet secure transaction protocols between merchants and customers, b) microtransactions – the Internet transaction of small monetary amounts.

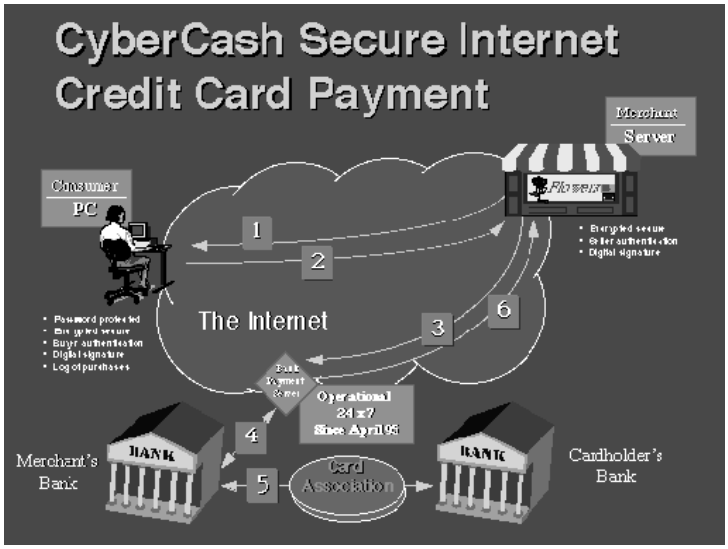

Figure 6: Procedures of CyberCash Exchange

5.2.1 CyberCash Secure Internet Credit Card Service

The CyberCash Secure Internet Credit Card Service provides a simple yet secure way of Internet purchasing with credit cards. See Figure 6. The CyberCash payment system consists of three parts: a "CC user software" on the user's machine, a "CC merchant software" on the merchant's machine, and the CyberCash server. When the user decides to buy, he uses the public key technology residing in his CC user software to encrypt his credit card information. The encrypted information along with the user's purchase authorization are then sent to the merchant. The merchant strips the purchase authorization from the message and adds on its identifier code to it and forwards it to the CyberCash server. The server decodes the the credit card information and merchant's code and performs the standard procedure of obtaining authorization from credit card companies. The server then passes the authorization back to the merchant, who sends a receipt to the user and ships the product.

Because only at the CyberCash server is the credit card information decoded, even the merchant cannot have access to the sensitive information. To intercept the information, the person must either decipher the public key technology encrypted code or monitor the process at the CyberCash server, neither of which is an easy task.

5.2.2 CyberCoin Service

The CyberCoin service enables transactions of small denominations on the Internet. In place of the CC user software in the Internet credit card service, the user uses a CyberCash wallet to purchase goods and services on the Internet. (See Figure 7). The user first downloads free CyberCash wallet software to his/her machine. To put money into the wallet, the user can either transfer money from his checking account of his bank or cash money using his credit cards. Equipped with money in the wallet, the user can buy goods and services from the Internet with denominations as small as \$0.25. Because the money in the wallet is pre-

approved, there is no need for the CyberCash server to obtain authorization from banking agencies or credit card companies during the purchase. As a result, neither the banking agencies nor the credit card companies keep records of individual purchases by the users; only the CyberCash wallet software keeps a log of all the transactions.

It is worth noting that CyberCoin is a notational system which means that the money is never moved onto or stored on the consumer's computer. When a consumer moves money into his/her wallet, a legal record of the money is created, but the real money resides in the domain of the banking systems. At the end of a business day, the funds between different accounts are reconciled within the banking networks. This contrasts with a tokenized system, where real e-money is being moved. This has important consequence in the event of a computer crash or malfunction. Because real money was never stored on the consumer's computer, instead of losing the digital money permanently, the consumer simply has to notify the CyberCash server of the computer crash and the money will be restored to his/her banking account.

This ease of monetary transaction enables purchasing of less substantial items like a New York Times article or a virtual tour of the Museum of Art. An example is the collaboration between CyberCash and Rocket Science Games. To play against players across the country in an interactive Internet game offered by Rocket Science, one will need to pay an entrance fee plus a small amount for every time increment. CyberCash provides the monetary modularity necessary for this type of applications.

5.2.3 Peer to peer payments

The ease of CyberCoin transaction permits users to transfer digital money from peer to peer directly. When a user wants to make a payment to another CyberCash account, the user simply sends an instruction to the CyberCash server to do so. The server will then check if the requested fund is legitimate and the instruction is not a duplicate. Then it updates both accounts and issues a signed receipt to the user. The user can then present the receipt to the payee as proof that the payment has been transfered. The payee can also contact the server and check the status of his account.

5.2.4 Message Format

Because there are many methods of sending information over the Internet, CyberCash needs a message format that is independent of the transmission mechanism. The CyberCash Version 0.8 General Message Wrapper Format is the following:

1. Header – denotes the start of a CyberCash message and includes version information.
2. Transparent Part – contains public information.
3. Opaque Part(s) – contains private information, such as financial information of the customer or the merchant. It is privacy protected and tamper protected.
4. Trailer – denotes the end of a CyberCash message. It also contains a check value so the receiver can determine if the entire message was received correctly.

Figure 7: Illustration of CyberCash Wallet

The Transparent Part and the Opaque Part are the sections that contains the important financial transaction information. The Transparent part includes information such as transaction number, local date and time at the requester's persona ID. The Opaque Part is always encrypted and contains sensitive information. The data is DES encrypted under a random transaction key, and the transaction key is RSA encrypted. A signature is generally not necessary if the message is a reply message; knowledge of the transaction key is enough of an authentication.

5.2.5 Security

As with any Internet payment systems, security is an important issue. CyberCash pays special attention to this issue and uses industrial strength encryption technology for protection against misappropriation. First, CyberCash uses Public Key encryption developed by RSA for authentication. The CyberCash server maintains records of the public keys associated with every customers and every merchants. The private key resides in the CC user software in the customer's computer and is only accessible only when a correct password is entered. Users are encouraged to store backup copies of their private keys at third party data recovery centers, in the event of a computer crash or accidental loss of data.

For encryption of the messages, it uses the Digital Encryption Standard (DES), commonly used in electronic payment system today. For very sensitive information such as PIN number, it may be superencrypted (i.e. encrypted more than one level). As a result, the plain text readable version of the information only exists temporarily; after it is read, it is immediately encrypted using another key.

5.2.6 RSA Encryption

As noted above, CyberCash uses RSA for public key encryption. The RSA algorithm was invented by Ron Rivest, Adi Shamir and Leonard Adleman in 1978. The following is the mathematical basis for the algorithm:

1. Find 2 large prime numbers, P and Q.
2. Choose E such that E and $(P-1)(Q-1)$ are relatively prime. i.e. the largest common factor between them is 1. Note that $(P-1)(Q-1)$ is even, and therefore it is not prime. As a consequence, E must be odd, but it does not have to be prime.
3. Compute D such that $(DE-1)$ is evenly divisible by $(D-1)(Q-1)$. D is called the multiplicative inverse of E.
4. The encryption function is $encrypt(T) = T^E \bmod PQ$, where T is the plaintext (a positive integer).
5. The decryption function is $decrypt(C) = C^D \bmod PQ$, where C is the ciphertext (a positive integer).

The public key is the pair (PQ, E), and the private key is the number D. PQ is the modulus, E is the public exponent, D is the secret exponent. Knowing only (PQ, E), it is very difficult to calculate D, P or Q. As a result, the tampering of private/public key pair is very unlikely.

5.2.7 Future

To compete with other Internet payment service providers, CyberCash, like its competition, needs to show that it has a dependable yet easy to use transaction system and a large body of merchants willing to use its service. At this juncture of this fast developing market, it is difficult to declare a winner.

References

[1] Nabil R. Adam, *Electronic Commerce: Current Research Issues and Applications* Nabil R. Adam, Yelena Yesha (eds.). Springer. New York. 1996.

[2] D. Barnes, "Identity Agnostic Online Cash", http://www.c2.net/ cman/agnostic.html

[3] A. Bhimani, "Securing the Commercial Internet", *Communications of the ACM*, pp. 29-35, June 1996.

[4] B. Boesch et al, "CyberCash Credit Card Protocol Version 0.8", *Network Working Group, Request for Comments: 1898*, February, 1996.

[5] Nathaniel S. Borenstein et al., "Perils and Pitfalls of Practical Cybercommerce", *Communications of the ACM*, Vol. 39 No. 6, pp. 36-44. June 1996.

[6] D. Chaum, "Achieving Electronic Privacy", *Scientific American*, August 1992, pp.96-101

[7] D. Chaum, "Security without Identification: card computers to make big brother obsolete", 1987, http://www.digicash.com/publish/bigbro.html

[8] Michael Krantz, "Cyber Vending Machine", *TIME* October 7 1996, pp. 78

[9] Levy, "Emoney (that's what I want)", *Wired*, December 1994, pp. 174-179 + 213-215

[10] B. C. Neuman and G. Medvinsky, "Requirements for Network Payment: The NetCheque Perspective", *Proceedings of IEEE Compcon '95*, pp. 32-36, March 1995.

[11] Patiwat Panurach, "Money in Electronic Commerce: Digital Cash, Electronic Fund Transfer, and Ecash", *Communications of the ACM*, Vol. 39 No. 6, pp. 45-50, June 1996.

[12] Marvin Sirbu and J. D. Tygar, "The NetBill Overview" *Proceedings of IEEE Compcon '95*, 1995.

[13] J. Swartz, "Encryption Technology For the Net: New method allows fearless transmissions", *San Francisco Chronicle*, p. D1, November 16, 1996.

[14] "About Ecash" http://www.digicash.com/ecash/about.htm