Digital Money
A divine gift or Satan's malicious tool?

Jörg Kienzle
jkienzle@di.epfl.ch

Adrian Perrig
aperrig@di.epfl.ch

STS Project*
EPFL Lausanne

April 22, 1996

Abstract

This document presents the advantages, but also the problems and dangers associated with a possible introduction of digital cash. After a brief review of the history of the monetary system in use today and a short introduction to cryptography, the key elements that should be considered when designing a digital cash system are discussed. The various attempts which are already practiced today and those which are currently in development are carefully analysed, highlighting their weaknesses and strengths. Finally, the advantages and disadvantages of electronic monetary systems are discussed.

*STS stands for Science Techniques Society

Contents

1 Prolog

The year is 2005. I wake up after a long dreamless night. My head feels still dizzy as I put on my clothes and prepare to leave my apartment. About to close the door, I suddenly realize that I forgot to take along my electronic wallet. I quickly open the drawer of my desk, grab it and put it into my inside pocket. Impatiently, I wait for the express elevator to surmount the 45 floors that separate me from the subway station.

At the gate, I type my personal identification number into my electronic wallet, which then contacts the ticket machine using an infra-red link to prove my identity and verify my subscription: access granted. Exhausted, I drop down on the first free seat. My thoughts deviate, the suburban landscape and the city traffic are passing by.

The rumbling of my stomach brings me back to reality. I get off the subway, enter my favorite fast-food restaurant and order a breakfast. The cashier gives me a choice of monetary units which are both displayed on the flat-panel screen for me to view. My scrambled eggs, ham and coffee will cost me US $50 or 5 pvu. The monetary symbol "pvu" is an abbreviation for "private value units", which now compete in most commercial settings with the US Dollar and have stayed remarkably stable since their initial issuance in mid-1996.

Having payed with wireless digital cash, I take a seat. The pressure in my stomach loses in strength, while I recall the old times, where people used to pay using real cash. Inconvenient and even dangerous, for everyone always had to carry some money around. Nowadays, nobody would steal your electronic wallet, since without the personal identification number it is useless. Besides, it is also tamper resistant and self-destructs if someone tries to get valuable information from it the hard way. I remember a scandal in 1999, when some American professor managed to break into one of the first electronic wallets by using high precision explosives and liquid nitrogen to freeze the contents of the memory right after opening the case before it could delete its contents. Fortunately, this problem has been fixed and the device is now considered perfectly secure.

I get up and leave the restaurant. Small refreshing raindrops fall on my face. Across the street, the administrative building of the DigiCash concern attracts all my attention. I have to be there at work in about 15 minutes. I dont need to hurry, there is still plenty of time.

2 Introduction

Throughout the last few years, personal computers have increasingly found their way into private homes. Many service providers offer modem access to the Internet, a world-wide network used to connect universities, but that now offers all kind of services and information to everyone. With the arrival of user-friendly, graphical browsers, small merchants saw their chance to advertise their goods. Slowly, commerce has found its way into the Internet.[1] Some way of payment over the net had to be found.

Of course, real money – the trillions of dollars handled each day by banks, other financial institutions, and government clearinghouses – is already digital. No physical tokens are exchanged: all transactions are conducted using streams of bits. But digitizing the final mile of electronic money will make all the difference in the world. It will not only change the physical way you spend your money, it will alter the way you view your own economic being. And depending on the manner in which it is implemented, digital money might allow others to view your financial status with a decidedly discomfiting intimacy.

The advent of high-quality color copiers threatens the security of paper money. The demand of guarding it makes paper money expensive. The hassles of handling it (such as vending machines) make paper money undesirable. The use of credit cards and ATM cards is becoming increasingly popular, but those systems lack adequate privacy or security against fraud, resulting in a demand for efficient electronic-money systems to prevent fraud and also to protect user privacy.

In order to clarify the important aspects that have to be considered when designing a digital cash system, section 3 will elucidate the history and use of ordinary money. Section 4 gives an introduction to cryptographic methods used in almost every current implementation of digital cash. In section 5 we will lay stress on the important key elements of an electronic monetary system. Then, we present an overview of some possible implementations of digital cash throughout section 6 and discuss their advantages and disadvantages in section 7 and section 8.

3 About Money

3.1 The History Of Money

The origin of money is shadowed in the dim ages of man's first feeble attempts at trading. Even primitive man must have found direct trading, or barter, an awkward and unsatisfactory expedient. If someone wanted to get an object a he had to find some other person who owned a and was willing to give it to him in exchange for an other object b, where both a and b had to be of equal value to each partner.

As man began to specialize his efforts he became increasingly dependent on some sort of market in which to dispose of the goods which he produced in excess of his consumption wants and to acquire the other goods he wanted to consume. Occasionally, he was forced, in order to make any trade at all, to accept some goods which he did not want for itself but which he knew someone else would be willing to accept in trade for something he did want. A series of such three party trades might well establish in each community the habit of looking upon some particular goods as widely enough acceptable to act as a satisfactory medium for execution of any exchange.

[1] You can now even order a pizza through the Internet.

The money idea might also have taken root in a slightly different way. A particular merchandise may have become generally acceptable due to its basic value, not with the idea of receiving and holding it between trades, but merely as a common denominator or standard against which to measure the value of both large (or intensely desired) things and small (or only slightly desired) things in working out the terms of a trade.

Whether money developed by the “medium of exchange” or by the “standard of value” route is of small consequence. In any economy that has progressed beyond the crudest stage the two functions are equally important, and any commodity that performs one satisfactorily is likely to be called upon to perform the other.

Traces of economic activity in the very earliest civilizations almost invariably show some commodity – cattle[2], grain, shells, trinkets, and the like – used as an exchange medium. With the passage of the centuries precious metals gained almost complete ascendancy over other commodities because they combined the attributes of portability, divisibility, durability, homogeneity, recognizability, stability of value, high value in small bulk, security and availability in reasonable amounts.

In the modern world convenience has been further enhanced by the growing acceptability of credit instruments, written promises to pay, represented by paper, plastic, or metallic tokens, as fully functional money with an exchange value clearly rated in terms of the basic unit of account, which is usually a fixed quantity of gold or silver. In the advanced money economy, therefore, goods and services are paid for not directly by other goods and services as in the barter economy, or even by commodities like gold or silver as in the early money economy, but by paper fiduciary moneys (checks, bank notes, government issues) which are offset against each other in the banking system, so that very little gold or silver needs to be transferred.

3.2 Disadvantages of barter

Under the primitive conditions of a barter economy, the services of all persons are exchanged directly, the master rewarding his servant with protection, food and shelter; and, between equals, goods of one kind are exchanged for goods of another kind. The dependence on chance coincidence makes barter an inadequate means of developing a market in which anyone can offer his goods with reasonable assurance of being able to trade for something else at least equal in utility for him.

Except in periods of crisis and confusion (i.e. WWII), barter has nowadays been replaced by money in the exchange of goods and services. Even in the barter arrangements themselves, money is commonly used as the unit of account by which the bartered products are evaluated. The money economy and the free market have replaced the barter economy because barter is burdensome, restrictive, and wasteful.

3.3 Advantages Of A Money Economy

In today's money economy increasing specialization is promoted by greater ease of exchange. The resulting economizing of skill and effort is one of the great blessings

[2] Camels in North Africa

that money has conferred on mankind.

A second aspect, of particular importance in a capitalistic society, is the automatic direction of the productive enterprise by the price system, which establishes the relative values of all goods and services and thereby largely determines what economic activities shall be pursued.

The third great benefit derived from the use of money is the availability of money loans whereby the producer may pay for his materials, machines, and labor before his own products reach the market. Large-scale productive enterprise could hardly function without available credit to support its development and sustain it when sales are low.

3.4 Money Standard

During the 19th century almost all countries adopted the gold standard. It served as a worldwide standard of value. This function was assumed by gold as a result of its attributes of portability, durability, divisibility, general desirability, stability in value, and high value in small bulk. We'll see later on that some of these features also have to be kept in mind when designing a digital money system.

The choice of the money system is an act of government by legislation or decree. In the system there is a standard money and a unit of account; all other moneys are multiples or subsidiaries of the standard unit. Provision is made for converting any type of money into any other. Coinage has become a state monopoly, and government further controls the money supply directly by legal-tender laws that define the moneys which a creditor must accept when offered by a debtor in settlement of a debt.

It should be clear that the actual circulating media of exchange, e.g., paper money and checks, need not themselves be the standard of value, but they must be expressed in terms of the standard of value in the unit of account, whatever the government may define that to be.

3.5 Electronic money

Until the last century, payments were generally made with coins and bank notes. Cash was also used as savings. Today, savings are rarely in cash. Wages are usually paid into a bank account. Many larger transactions, such as rent, insurance and tax payments, are paid with cheques or transfer orders, or they are paid electronically as standing orders and direct debits.

With the emergence of electronic funds transfer for payments at the point of sale, the credit card, a small card containing a means of identification, such as a signature or picture, became increasingly widespread. It authorizes the person named on it to charge goods or services to his account, on which he is billed periodically.

The use of credit cards originated in the United States during the 1920s, when individual firms, such as oil companies and hotel chains, began issuing them to customers for purchase made at company outlets.

Finally, the bank system adopted credit cards. It credits the account of the merchant as sales slips are received and assembles the charges to be billed at the end of the period to the card holder, who pays the bank. The card holder may choose to pay on an installment basis, in which case the bank earns interest on the outstanding balance. The interest income permits banks to refrain from charging card holders an annual fee and to charge participating merchants a lower service charge. An additional advantage of the system is that merchants receive their payments promptly by depositing their bills of sale with the bank.

3.6 Confidence, A Key Element

Commodity money circulates because the stability of the society gives ground for confidence that the money will continue to be accepted habitually in exchange for goods and services. Similarly, the credit instruments of any government, bank, corporation, firm, or individual will circulate more or less widely in proportion to public confidence in its promises to pay. Likewise, a possible introduction of a digital cash system will require a period of long-term trust.

4 Introduction to Cryptography

Cryptography is used in most digital money schemes in many different ways. Here are a few examples:

- Authenticate the user to the bank.
- Money can be generated by banks, represented by a long number.
- Nobody except the bank can alter the number representing the value, without the "bill" losing its value.
- Send data safely over a public phone line or the Internet. An eavesdropper can not use, read or understand that data.
- Digital signatures.

This section introduces the basic concepts and underlying principles of cryptography. Unfortunately, a profound mathematical knowledge is required to understand section 4.2 up to section 4.3. In case you would like to skip this part, the important concepts introduced are:

- RSA is a public key cryptographic algorithm. This means that everybody on the planet can encrypt a message to Alice with Alice's public key, but only Alice will be capable of decrypting the message, by using its secret key. It is important to note that there are 2 different keys that form a pair, one is public and is used to encrypt a message and the private key is kept secret, so only the receiver can decrypt the message. Every person has a unique keypair.
- DES is a private key algorithm. If Bob and Alice want to exchange encrypted information, they both need to possess one private key, which is kept secretly between them. This key is needed for both encryption and decryption of the message.

- Digital Signatures can be used to uniquely sign an electronic document. Similar to the RSA public key algorithm, but this time using the private key, Alice will compute a number representing the signature of the document, which depends on the document content as well as Alice's private key. Everybody can now verify, by using Alice's public key, that really Alice wrote the document and that the document was not altered by anybody after the computation of the signature.

4.1 Encryption Systems

An encryption system is a procedure which takes the original message (*plaintext*) and a small piece of information arranged in advance between sender and receiver (the *key*) and creates an encoded version of the message (the *ciphertext*[3]).

When we are considering the quality of an encryption system, we assume the person trying to decode the message knows what the general procedure is and is looking at the ciphertext— the only thing he does not have is the key. We also assume the person sending messages does not spend time trying to contrive a difficult-to-read message by using unusual words or letter frequencies— the sender is counting on the system to provide all the needed security.

Usually one assumes the person trying to break the code is only working with the ciphertext. However, there are situations in which both plaintext and ciphertext of a previously encoded message are available. One countermeasure against this type of *known-plaintext attack* is to continually change keys, assuming an encryption using one key is not helpful for attacking a message using a different key. It can become difficult to keep track of the different keys in use, especially if they are long.

A more demanding standard is that a code may be safe against a *chosen-plaintext attack*. We are imagining that the encryption is done by a machine, and that unauthorized persons may have access to the machine (although we assume they are only using it in the normal way, not allowed to take it apart).

Example 1: Simple Substitution

This is the simple letter-for-letter method found in Poe's "The Gold Bug" and many other stories. The key is a rearrangement of the 26 letters:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
actqgwrzdevfbhinsymujxplok
```

Using this key, the plaintext:

```
THE SECURITY OF THE RSA ENCODING SCHEME RELIES ON THE
FACT THAT NOBODY HAS BEEN ABLE TO DISCOVER HOW TO TAKE
CUBE ROOTS MOD N WITHOUT KNOWING NS FACTORS
```

becomes the ciphertext:

[3] A cipher is a method of cryptography by applying an algorithm to the letters or digits of the plaintext [DP92].

```
UZG MGTJYDUO IW UZG YMA GHTIQDHR MTZGBG YGFDGM IH UZG
WATU UZAU HICIQO ZAM CGGH ACFG UI QDMTIXGY ZIP UI UAVG
TJCG YIIUM BIQ H PDUZIJU VHIPDHR HM WATUIYM
```

The messages can be made harder to decode (but also harder to read!) by leaving out the spaces between words.

Most messages can be decoded by looking for frequently occuring pairs of letters (TH and HE are by far the most common), using these to identify a few letters to begin, and filling in the remaining letters one at a time ("The Gold Bug" gives a good description, as do many books).

In a known-plaintext situation, the whole code is obtained almost immediately. However, in our example, the letters J, P, and others do not occur in the plaintext, so we could not tell how they are encoded. If we were allowed a chosen plaintext, we would use all the letters to get the entire key.

Example 2: The Vigenère cipher and one-time pads

This cipher works by replacing each letter by another letter a specified number of positions further in the alphabet. For example J is 5 positions further than E. D is 5 positions after Y. (Y,Z,A,B,C,D) The key is a sequence of shift amounts. If the sequence is of length 10, the 1st, 11th, 21st, ... letters of the plaintext are processed using the first member of the key. The second member of the key processes plaintext letters 2, 12, 22, ... and so forth. If we omit spaces from the plaintext on page 6 and use the key-sequence:

3 1 7 23 10 5 19 14 19 24

we obtain

```
WILPOHNFBR BPMQRJKGTC QDVASSZGVF
HNLOOQBSLM QUOBPFVHMF DUULLTWMAY VCLBXFUZXR
REPPMTOSKF RXALDFDSVS EFYLYYLAHB QXPQRTNHDL
RXPKQSLTTA WPYP
```

(We have divided the ciphertext into groups of ten letters for convenience. The division into lines is arbitrary.)

This type of cipher was considered very secure at one time ($\sim$ 1600), but is not really difficult. Suppose we guess that the first letter is T. This implies the eleventh letter is Y, the 21st letter is N, etc. Now look at the two-letter combinations that occur from different possibilities for the second letter:

```
TI YP ND EN NU AU SC OE OX BF NX OX TP   (no shift of 2nd letter)
TJ YQ NE EO NV AV SD OF OY BG NY OY TQ
TK YR NF EP NW AW SE OG OZ BH NZ OZ TR
TL YS NG EQ NX AX SF OH OA BI NA OA TS
   (skipping over some in the middle)
TF YM NA EK NR AR SZ OB OU BE NU OU TM
TG YN NB EL NS AS SA OC OV BD NV OV TN
TH YO NC EM NT AT SB OD OW BE NW OW TO
```

The last line is the "right answer." Although it shows several bad combinations (`NC NT SB NW`), mostly caused by the last letter of one word being adjacent to the first letter of the next word, it looks better than the other possible rows. Once the second letter has been identified, the same approach can be used to get the third letter. This approach is easily automated using a table of digrams.

It is necessary to know the first letter and the length of the key-sequence. If we assume the length is not too large, a program can just try all possibilities, eventually choosing the plaintext which looks best.

One-time pads A long key-sequence makes this approach more difficult, since we have fewer rows. The extreme case is that in which the key-sequence is as long as the plaintext itself. This leads to a theoretically *unbreakable* cipher. For any possible plaintext, there exists a key for which the given ciphertext was derived from that plaintext.

This type of cipher has reportedly been used by spies, who were furnished with notebooks containing page after page of randomly generated key-sequence. Notice that it is essential that each key-sequence is used only once (hence the name of the system). Otherwise the approach for Vigenère systems described above could be tried, since we would have at least two rows to work with.

One-time pads seem practical in situations where one agent is communicating with a central command. They become less attractive if several agents may need to communicate with each other. The one-time feature is lost if X and Y inadvertently use the same page to talk as W and Z are using. Also capture of X's equipment makes it possible to overhear a conversation between Y and Z.

Example 3: A Transposition System

In this system, we will assume that every line of the message is 63 characters long. The key is a permutation of the numbers from 1 to 63, and each line of the plaintext is rearranged using the permutation to produce the corresponding ciphertext. For example if the key is

$$1\ 11\ 21 \ldots 61\ 8\ 18 \ldots 54$$

(we would really want to use a more complicated permutation) and we use the same plaintext as in the previous two examples, we obtain:

```
TTRNRT UHOMO SFECE HYSGEH REDEN E NHS E A LE I I   CTCE   O SI
FN  ET AHBCT  DNDO AOBTRA TALOO TY IW CBEO K  SEV  H AS  TOE HE
C HNO  OWOA     S  UMOGR  TIWC  RNK   BOU S  STIT  O NF  EDTN
```

We are using the version of the plaintext including blanks. The second line of the plaintext has 55 characters, so we add 8 blanks on the end.

One method of decoding looks at a column of the ciphertext and asks what other column could immediately follow it. For example, it is possible that the column following `OBO` (the tenth ciphertext column) is `UAO` (the 8th), but the column `TFC` would yield the improbable two-letter combination `BF`.

As always, a longer message is easier to decode. Unlike simple substitution, it seems that blanks make the decoding process more difficult.

What about a known-plaintext attack? Since there is only one Y in the first line of the plaintext, we can tell that column 12 of the plaintext is column 21 of the ciphertext, but there are other things we can't tell. In this example, there are 8 columns of three blanks at the end of the plaintext, and we can't be sure which of these corresponds to which of the all-blank ciphertext columns. (it doesn't matter for this message, but we would like to know the entire key to deal with longer plaintexts in the future) A carefully chosen plaintext can give us the entire key at once.

4.2 Introduction to Number Theory

In order to explain the basic concepts of the RSA algorithm, which is used in most digital money schemes, we must first introduce some mathematical notions and theorems.

4.2.1 Congruences

The congruence $a \equiv_n b$ ("a is congruent to b mod n") says that, when divided by n, a and b have the same remainder.

$$100 \equiv_{11} 34 \qquad -6 \equiv_8 10$$

In the second congruence, we are using $-6 = 8(-1) + 2$. We always have $a \equiv_n b$ for some $0 \leq b \leq n-1$, and we are usually concerned with that b. If $a \equiv_n b$ and $c \equiv d$, we can add or multiply

$$a + c \equiv_n b + d \qquad ac \equiv_n bd$$

Division does not always work: $6 \equiv_{12} 18$ but $3 \not\equiv 9$.

4.2.2 The Greatest Common Divisor

For a and b, the number (a, b) is the largest number which divides a and b evenly.

$$(56, 98) = 14 \qquad (76, 190) = 38$$

Theorem 1 *For any a, b there are integers x, y with $ax + by = (a, b)$*

This can be seen by solving the equation by making a sequence of simplifying substitutions:

$$\begin{array}{rcll} 30x + 69y & = & 3 & \\ 30x' + 9y & = & 3 & [x' = x + 2y] \\ 3x' + 9y' & = & 3 & [y' = y + 3x'] \\ 3x'' + 0y' & = & 3 & [x'' = x' + 3y'] \end{array}$$

It is easy to see that $x'' = 1$, $y' = 0$ is a solution to the final equation and we get a solution to the original equation by working backwards:

$$x' = x'' - 3y' = 1 \quad y = y' - 3x' = -3 \quad x = x' - 2y = 7$$

We could also solve an equation like $30x + 69y = 15$ by multiplying our solution: $y = -15$, $x = 35$. It should be clear that the equation will have no solution in integers if 15 is replaced by something that is not a multiple of $(30, 69) = 3$.

All other integer solutions of $30x + 69y = 15$ may be obtained by changing the first solution:

$$y = -15 + \frac{30}{3}t \quad x = 35 - \frac{69}{3}t \quad \text{for } t \text{ integer}$$

If we do the process illustrated on the previous page for any equation $ax + by = (a, b)$, we eventually get one of the coefficients as zero and the other as (a, b). In fact, this process is usually presented as "Euclid's algorithm for finding the greatest common divisor."

It is important that this process is feasible on a computer even if a and b are several hundred digits long. It is easy to show that the larger of the two coefficients decreases by at least 1/2 every two equations, hence every twenty equations the larger coefficient has decreased by $2^{-10} < 10^{-3}$, so a 600-digit number would not require more than 4000 equations.

We pointed out earlier that division does not work with congruences. An important application of Theorem 1 is that it does work for prime numbers.

Corollary 2 *If p is a prime number, $ar \equiv_p as$ and $a \not\equiv 0$, then $r \equiv s$.*

Corollary 3 *If p is a prime number and $a \not\equiv 0$ mod p, then for any b, there is y with $ay \equiv_p b$.*

Corollary 4 (The "Chinese Remainder Theorem") *If $(p, q) = 1$, then for any a, b, there is an n with*

$$n \equiv_p a \quad \textit{and} \quad n \equiv_q b$$

4.2.3 Powers modulo a prime

The sequence

$$a \quad a^2 \quad a^3 \ldots \quad \text{mod } p$$

has many applications in cryptography. Before looking at theoretical properties, the example below (done using a pocket calculator) should make clear that it is practical to compute these numbers, even when many digits are involved.

Suppose we want to compute 432^{678} mod 987. The basic trick is to start with a number and keep squaring:

$$432^2 = 186624 \equiv 81 \quad 432^4 \equiv 81^2 \equiv 639 \quad 432^8 \equiv 639^2 \equiv 690 \ldots 432^{512} \equiv 858$$

Since $678 = 512 + 128 + 32 + 4 + 2$,

$$432^{678} \equiv (81)(639)\ldots(858) \equiv 204$$

Calculations with exponents involve not-too-many multiplications. If the numbers have several hundred digits, however, it is necessary to design special subroutines to do the multiplications [Knu81].

Let us look at the sequence of powers of 2 mod 11:

$$2\ 4\ 8\ 5\ 10\ 9\ 7\ 3\ 6\ 1$$

Each number from 1 to 10 appears in the sequence.

Theorem 5 *Let p be a prime. There is an a such that for every $1 \leq b \leq p-1$, there is $1 \leq x \leq p-1$ such that $a^x \equiv_p b$.*

It is not always the case that $a = 2$. The powers of 2 mod 7 are 2, 4, 1 after which the sequence repeats and we never get 3, 5, or 6.

Let's look at some of the consequences of Theorem 5.

Corollary 6 *Let a be as in Theorem 5. Then $a^{p-1} \equiv_p 1$.*

Corollary 7 *For any $b \not\equiv 0$, $b^{p-1} \equiv_p 1$.*

Corollary 8 *If $x \equiv_{(p-1)} y$, then $b^x \equiv_p b^y$*

Lemma 9 *Let $b \not\equiv 0$, d the smallest positive number such that $b^d \equiv 1$. Then for any $e > 0$ with $b^e \equiv 1$ d divides e evenly. In particular, by Corollary 7, d divides $p-1$ evenly.*

4.2.4 Primitive roots

Theorem 5 showed that if p is a prime, there is an a such that the equation

$$a^x \equiv_p b$$

has a solution for any $b \not\equiv 0$. Such an a is called a *primitive root* of p, and x is called the *discrete logarithm* of b.

We showed in subsection 4.2.3 that it is easy to obtain b given a and x. Finding x given a and b is much harder. Many modern encryption systems are based on the fact that no efficient way of computing discrete logarithms is known.

Neither an efficient method for always finding primitive roots is known. However, it is often possible to find one in special cases. We will use $p = 1223$ as an example. $p - 1 = 2 \cdot 13 \cdot 47$. By Lemma 9, if a is not a primitive root, then we will either have a^{26}, a^{94}, or $a^{611} \equiv_{1223} 1$. $a = 2$ and 3 fail, but $a = 5$ satisfies all three conditions, so it is a primitive root. We could tell that $a = 4$ would not be a primitive root without testing.

It is easy to show that, if a is a primitive root, a^x is a primitive root if and only if $(x, p-1) = 1$. In this example, this means the number of primitive roots is

$$1222\left(\frac{1}{2}\right)\left(\frac{12}{13}\right)\left(\frac{46}{47}\right) = 552$$

Thus, if we had just chosen a at random, the probability that it would be a primitive root is $\approx .45$. Choosing a at random and testing until we found a primitive root would not be expected to take too long.

This is an example of a *probabilistic algorithm.* It is possible for it to take a long time, but the amount of time needed on average is reasonably small. We will see many other probabilistic algorithms later.

4.3 Encryption based on powers and congruences

4.3.1 The Diffie-Hellman key exchange procedure

A and B are communicating. C hears everything A and B say. A and B want to agree on a number, without C knowing what the number is. It may be, for example, that A and B plan to use the number as the key for future encoded messages. The procedure (also often called a *protocol*):

A and B agree on a (large) prime p and a primitive root a. These numbers are also known to C. A secretly chooses a (large) number X_1, B secretly chooses X_2. a^{X_1} and a^{X_2} mod p are publicly announced (hence known to C). The secret number will be $S = a^{X_1 X_2}$ mod p.

$$\text{A calulates } S \equiv \left(a^{X_2}\right)^{X_1} \qquad \text{B calculates } S \equiv \left(a^{X_1}\right)^{X_2}$$

A possible drawback to this system is that neither A nor B controls what S is. If S is not a satisfactory[4] number, they may have to repeat the protocol.

Diffie and Hellman suggest the procedure can also be used in a situation in which n people must find, for each pair of people, an agreed-upon number. For $1 \leq i, j \leq n$ the number is $a^{X_i X_j}$.

4.3.2 The Rivest-Shamir-Adleman public key system

A sets up a system so that anyone can send him an encoded message, but only A will be able to decode it. The message is represented as a number M. The encoding is done by a publically known function $f(M)$, with A the only person who knows how to compute f^{-1}. A chooses two large primes p, q which he keeps secret. He announces $n = pq$ and another number d, with $(d, p-1) = (d, q-1) = 1$ (one way to do this is to choose d a prime larger than $p/2$ and $q/2$.) The encoding is

$$f(M) \equiv M^d \text{ mod n}$$

where M and $f(M)$ are both $\leq n-1$. As we have seen f can be computed in a realistic amount of time even if M, d, n are many digits long.

[4]For several ciphers, weak numbers exist, for which the complexity to break the ciphertext is relaxed.

A computes M from M^d using his knowledge of p, q. By Corollary 8,

$$\text{If } de \equiv_{(p-1)} 1 \text{ then } \left(M^d\right)^e \equiv_p 1$$

Similarly $\left(M^d\right)^e \equiv_q M$ if $de \equiv_{(q-1)} 1$. e satisfies these two conditions if $ed \equiv_{(p-1)(q-1)} 1$. Theorem 1 says we can let $e = x$, where x is a solution of

$$dx + (p-1)(q-1)y = 1$$

Since $\left(M^d\right)^e - M$ is divisible by p and by q, it is divisible by pq, hence we can recover M from M^d by taking to the e-th power mod pq.

It is crucial to the security of this system that knowledge of n does not allow an eavesdropper to calculate p and q. The crude approach of dividing n by all numbers up to $\sqrt{n}$ would take $\sim 10^{50}$ steps for a 100-digit n. However, many famous mathematicians have been unable to devise significantly better factoring algorithms, and this problem has been studied for at least 100 years.

One practical difficulty in using this system is the need to do calculations with many-digit numbers, especially to find primes. Another difficulty is that the inventors of this system have patented it. Amateur programmers who have posted implementations on electronic bulletin boards have received letters from "RSA Security, Inc" warning of possible patent infringement.

4.3.3 A public key system as hard as factoring

It is possible in theory that there is some way of computing f^{-1} for the system in the previous section that does not involve determining p and q. In the original RSA paper [RSA78], the authors say

> It may be possible to prove that any general method of breaking our scheme yields an efficient factoring algorithm. This would establish that any way of breaking our scheme must be as difficult as factoring. We have not been able to prove this conjecture, however.

To see the difficulties involved in trying to prove such a thing, suppose that one could show that knowledge of a ciphertext $f(M)$ and a plaintext M enabled one to find p and q. Then one could factor n as follows:

1. Choose any M.
2. Compute $f(M)$. (Remember, we are assuming f is publicly available. Furthermore, $f(M)$ can't be too hard to compute, or the code would be impractical.)
3. Use the assumed method to obtain p, q.

In words, we are unable to distinguish between the situation in which $f(M)$ is obtained from M (easy) and the (presumably difficult) situation in which M is obtained from $f(M)$.

Rabin has suggested an alternative to the RSA system in which there is a direct connection to factoring. As in RSA, $n = pq$ is announced publicly, with primes p, q kept secret. For technical reasons, we assume $p, q \equiv_4 3$. The encoding function is

$$f(M) \equiv_n M^2$$

The way we avoid the difficulty described above is that there are *four* numbers M_1, M_2, M_3, M_4 with $f(M_i) \equiv f(M)$. The key facts are:

1. If p, q are known, it is easy to compute all the M_i given $f(M)$.
2. If we are given n, $f(M)$, and all the M_i, we can calculate p, q.

We are *not* able to obtain p, q from just one of the M_i, so the approach based on M and $f(M)$ described above won't work. One drawback of this system is that, even with knowledge of p and q, one can only say the number sent is one of the four M_i, without being able to identify which one. In practice, this is not serious, since it is very unlikely that more than one of the M_i would correspond to a feasible message.

Unfortunately, this cryptosystem is vulnerable to a chosen-plaintext attack, even if we assume that the person trying to break the code gets only one of the M_i, chosen randomly. The attacker keeps generating pairs M, $f(M)$ until he gets an M_i with $(M + M_i, n) = p$ or q.

4.4 Product Ciphers

A product cipher is a block cipher that iterates several weak operations such as substitution, transposition, modular addition/multiplication, and linear transformation. (A "block cipher" just means a cipher that encrypts a block of data—8 bytes, say—all at once, then goes on to the next block.) The notion of product ciphers is due to Shannon.

Nobody knows how to prove mathematically that a product cipher is completely secure. So in practice one begins by demonstrating that the cipher "looks highly random". For example, the cipher must be nonlinear, and it must produce ciphertext which functionally depends on every bit of the plaintext and the key. It was shown that at least 5 iterations of DES are required to guarantee such a dependence. In this sense a product cipher should act as a "mixing" function which combines the plaintext, key, and ciphertext in a complex nonlinear fashion.

The fixed per-round substitutions of the product cipher are referred to as S-boxes. For example, LUCIFER[5] has 2 S-boxes[6], and DES has 8 S-boxes. The nonlinearity of a product cipher reduces to a careful design of these S-boxes.

[5] LUCIFER was the predecessor of DES and was developed by IBM in the early 1970s.

[6] An S-Box is a substitution operation which scrambles the input string (changes the position of the bytes)

4.4.1 DES

The first public algorithm that solved many of the problems[7] was introduced in 1975 by IBM, the National Security Agency (NSA), and the National Bureau of Standards (NBS) (now called NIST). This algorithm was simply known as the Data Encryption Standard, or DES. DES is the U.S. Government's Data Encryption Standard, a product cipher that operates on 64-bit blocks of data, using a 56-bit key. Instead of defining just one encryption algorithm, DES defines a whole family of them (several quadrillion, in fact). With a few exceptions, a different algorithm is defined for each number less than 2^{56}.

This means that everybody can be told about the algorithm and your message will still be secure. This makes your secret key much smaller. It is no longer necessary to send a copy of your algorithm to each person you want to communicate with. You just need to tell them your secret key, a number less than 2^{56}. The number 2^{56} is also large enough to make it difficult to break the code using a brute force attack (i.e., trying to break the cipher by using all possible keys).

DES has withstood the test of time. Despite the fact that its algorithm is well known, it is impossible to break the cipher without using tremendous amounts of computing power. If you use DES three times on the same message with different secret keys, it is virtually impossible to break it using existing algorithms. Over the past few years several new, faster symmetric algorithms have been developed, but DES remains the most frequently used.

4.5 Message Digest and Digital Signatures

A typical one-way hash function or message digest function takes a variable-length message and produces a fixed-length hash. Given the hash it is computationally impossible to find a message with that hash; in fact one can't determine any usable information about a message with that hash, not even a single bit. For some one-way hash functions it's also computationally impossible to determine two messages which produce the same hash.

A one-way hash function can be private or public, just like an encryption function. Here's one application of a public one-way hash function, like MD5 or Snefru. Most public-key signature systems are relatively slow. To sign a long message may take longer than the user is willing to wait. Solution: Compute the one-way hash of the message, and sign the hash, which is short. Now anyone who wants to verify the signature can do the same thing.

In practice, the public key is placed in a public database known as a key server. Whenever somebody wants to find out what your public key is, they send a request to the key server. So if somebody wanted to find out Mr. X's public key, they would send a request to the key server and get back something like "Mr. X's public key is 3A197BC2" (real public keys are actually far longer than this). Now everybody knows two things:

[7] The requirements were a high level of security, completely specified and easy to understand, economical to implement and efficient to use, among other reasons.

If you want to send me a message that only I can read, all you have to do is encrypt it with 3A197BC2.

If you receive a message that can be decrypted with 3A197BC2, it must have come from me.

This second point is very important. It allows a user to make "digital signatures." Just like physical signatures, digital signatures are a method of guaranteeing somebody's identity. As long as you don't let anybody know what your private key is, it will take impossibly large amounts of computing power to "forge" your digital signature. It is an extremely good idea to "sign" electronic documents by using your private key to encrypt the "message digest" of the document. A message digest is a relatively short block of numbers that prevents anybody from altering your document. Changing even a single letter would cause the message digest to become completely different.

4.6 Methods Of Attack

A standard cryptanalytic attack is to know some plaintext matching a given piece of ciphertext and try to determine the key which maps one to the other. This plaintext can be known because it is standard (a standard greeting, a known header or trailer, ...) or because it is guessed. If text is guessed to be in a message, its position is probably not known, but a message is usually short enough that the cryptanalyst can assume the known plaintext is in each possible position and do attacks for each case in parallel. In this case, the known plaintext can be something so common that it is almost guaranteed to be in a message.

A strong encryption algorithm will be unbreakable not only under known plaintext (assuming the enemy knows all the plaintext for a given ciphertext) but also under "adaptive chosen plaintext" – an attack making life much easier for the cryptanalyst. In this attack, the enemy gets to choose what plaintext to use and gets to do this over and over, choosing the plaintext for round N+1 only after analyzing the result of round N.

For example, as far as we know, DES is reasonably strong even under an adaptive chosen plaintext attack (the attack Biham and Shamir used). Of course, we do not have access to the secrets of US government cryptanalytic services. Still, it is the working assumption that DES is reasonably strong under known plaintext and triple-DES[8] is very strong under all attacks.

To summarize, the basic types of cryptanalytic attacks in order of difficulty for the attacker, hardest first, are:

- **ciphertext only:** the attacker has only the encoded message from which to determine the plaintext, with no knowledge whatsoever of the latter. A ciphertext only attack is usually presumed to be possible, and a code's resistance to it is considered the basis of its cryptographic security.
- **known plaintext:** the attacker has the plaintext and corresponding ciphertext of an arbitrary message not of his choosing. The particular message of the

[8]Triple-DES is implemented by applying 3 times DES to the data.

sender is said to be 'compromised'. In some systems, one known ciphertext-plaintext pair will compromise the overall system, both prior and subsequent transmissions, and resistance to this is characteristic of a secure code.

Under the following attacks, the attacker has the far less likely or plausible ability to 'trick' the sender into encrypting or decrypting arbitrary plaintexts or ciphertexts. Codes that resist these attacks are considered to have the utmost security.

- **chosen plaintext:** the attacker has the capability to find the ciphertext corresponding to an arbitrary plaintext message of his choosing.
- **chosen ciphertext:** the attacker can choose arbitrary ciphertext and find the corresponding decrypted plaintext. This attack can show in public key systems, where it may reveal the private key.
- **adaptive chosen plaintext:** the attacker can determine the ciphertext of chosen plaintexts in an interactive or iterative process based on previous results. This is the general name for a method of attacking product ciphers called 'differential cryptanalysis'.

4.6.1 Differential Cryptanalysis

Differential Cryptanalysis is a statistical attack that can be applied to any iterated mapping (i.e., any mapping which is based on a repeated round function). The method was recently popularized by Biham and Shamir, but Coppersmith has remarked that the S-boxes of DES were optimized against this attack some 20 years ago. This method has proved effective against several product ciphers, notably FEAL.

Differential cryptanalysis is based on observing a large number of ciphertexts Y, Y' whose corresponding plaintexts X, X' satisfy a known difference $D = X + X'$, where $+$ is component-wise XOR. In the basic Biham-Shamir attack, 2^{47} such plaintext pairs are required to determine the key for DES. Substantially fewer pairs are required if DES is truncated to 6 or 8 rounds. In these cases, the actual key can be recovered in a matter of minutes using a few thousand pairs. For full DES this attack is impractical because it requires so many known plaintexts.

The work of Biham and Shamir on DES revealed several startling observations on the algorithm. Most importantly, if the key schedule was removed from DES and a 16*48 = 768-bit key was used, the key could be recovered in less than 2^{64} steps. Thus independent subkeys do not add substantial security to DES. Further, the S-boxes of DES are extremely sensitive in that changing even single entries in these tables yields significant improvement in the differential attack.

Adi Shamir is quoted to say (NYTimes Oct 13 1991), "I would say that, contrary to what some people believe, there is no evidence of tampering with the DES so that the basic design was weakened."

5 Key Elements of a Digital Cash System

Before we will explain how digital cash could be implemented, we would like to point out some important key elements that should be considered when analyzing the different methods. Each property is illustrated by a small example.

5.1 Mandatory Properties

5.1.1 Security

Alice should be able to pass digital cash to Bob without that either of them, or others, can alter or reproduce the electronic token.

The transaction protocol must ensure that a high-level security is maintained through sophisticated encryption techniques. The communication can be made secure using private key encryption, whereas the authentication of sender and receiver can be accomplished using digital signatures. Online verification can prevent double-spending, or other off-line techniques must be used.

5.1.2 User-friendly

Alice and Bob should not require an advanced degree in cryptography as the protocol machinations should be transparent to the immediate user.

The digital cash should be simple to use from both the spending perspective and the receiving perspective. Complicated systems are difficult to administer and raise the failure rate due to errors of the user. Simplicity leads to mass use and mass use leads to wide acceptability.

5.1.3 Portable

Alice and Bob should be able to walk away with their digital cash and transport it within alternative delivery systems, including non-computer-network delivery channels.

The security and use of digital cash should not be dependent on any physical location. The cash can be transferred through computer networks and off the computer network into other storage devices. Digital wealth should not be restricted to a unique, proprietary computer network.

5.1.4 Two-way and Transferability

Alice, Bob, Carol, and David share an elaborate dinner together at a trendy restaurant and Alice pays the bill in full. Bob, Carol, and David each should then be able to transfer one-fourth of the total amount in digital cash to Alice.

The digital cash should be transferable to other users. Essentially, peer-to-peer payments are possible without either party required to attain registered merchant status as with today's card-based systems.

This is a very important element if digital cash is to replace ordinary cash. Think of situations where you hand money personally to someone else, e.g. as a gift, as charity, or as a tip. It is important to waiters to have some means to supplement low pay.

There are also other person-to-person payments for which only cash is regarded appropriate, like payments to children, friends, colleagues or neighbors.

5.2 Desired Elements

5.2.1 Off-line Capable

Alice can freely pass value to Bob at any time of day without requiring third-party authentication.

The protocol between the two exchanging parties is executed off-line, meaning that neither is required to be host-connected in order to process. Availability must be unrestricted.

5.2.2 Divisible

Alice and Bob should be able to approach a provider or exchange house and request digital cash breakdowns into the smallest possible units. Or Alice should be able to sign some sort of check and fill in the amount of money that she wants to pay to Bob.

In the first approach, a digital cash token in a given amount can be subdivided into smaller pieces of cash in smaller amounts. The cash must be fungible so that a reasonable portions of change can be made. The smaller the better to enable high quantities of small-value transactions.

The second approach would require special encryption techniques to allow filling in the amount of money that you want to pay onto some sort of digital check. A check would be certified from the bank up to a certain value. This kind of approach could not be anonymous, for the bank must know who issued the check in order to debit the amount of money that he has spent from his account.

5.2.3 Infinite Duration

Alice should be able to store a token somewhere safe for ten or twenty years and then retrieve it for use.

The digital cash should not expire. It should maintain its value until lost or destroyed provided that the issuer has not debased the unit to nothing or gone out of business. Without this property, people would want to keep all their money in bank accounts or cash and only use digital cash if they have to.

5.2.4 Wide Acceptability

Alice should be able to pay using digital cash in any situation, for small purchases (like buying a hot-dog) as well as for bigger ones (e.g. buying a car).

Digital cash should become well-known and accepted in a large commercial zone. Primarily a brand issue, this feature implies recognition of and trust in the issuer. Even with several digital cash providers displaying wide acceptability, Alice should be able to use her preferred unit in more than just a restricted local setting.

5.2.5 No Secret Algorithm

Alice and Bob should be able to get hold of a complete description of the algorithm used to ensure safety in the digital money system in a legal way.

The security of digital money should not depend on the secrecy of the algorithm used to manufacture or transfer money. Thus, giving everybody the possibility to verify and check the correctness and strength of the used cipher, such a system will inspire overall confidence. At the same time, everyone is able to write software for all electronic devices that can be found in such a system, making manufacturing monopoly and special security measures obsolete.

5.3 Optional Properties

5.3.1 Anonymity

Both Alice and Bob should have the option to remain anonymous in relation to the payment. Furthermore, at the second level, they should have the option to remain completely invisible to the mere existence of a payment on their behalf.

Anonymity ensures the privacy of a transaction on multiple levels. Beyond encryption, this optional untraceability feature of digital cash promises to be one of the major points of competition as well as controversy between the various providers. Transactional privacy will also be at the heart of the government's attack on digital cash because it is that feature which will most likely render current legal tender irrelevant.

If digital currency were fully untraceable, it would open up opportunities for abuse that are not available to criminals now. In the physical world, money is bulky. In the physical world, it is possible to follow people, so a kidnaper can potentially be caught if the currency is marked, if the money was being observed on location, or if the serial numbers were recorded. Fully anonymous cash might allow opportunities for counterfeiting and fraud.

On the other hand, traceable digital cash would give enormous power to the government and the credit agencies. Currently, credit card charges can be monitored and compiled to create a portfolio on you and all of your purchases. Cash is free from this threat. With non-anonymous electronic cash, there is the fear that ALL transactions will be recorded, and that consumers will lose all purchasing privacy.

Already, public and private sector organizations acquire extensive personal information and exchange it amongst themselves. Individuals have no way of knowing if this information is inaccurate, outdated, or otherwise inappropriate, and may only find out when they are accused falsely or denied access to services. New and more serious dangers derive from computerized pattern recognition techniques: even a small group using these and tapping into data gathered in everyday consumer transactions could secretly conduct mass surveillance, inferring individuals' life-styles, activities, and associations. The automation of payment and other consumer transactions is expanding these dangers to an unprecedented extent.

5.3.2 Unit-of-value Freedom

Alice and Bob should be able to issue non-political digital cash denominated in any defined unit which competes with governmental-unit digital cash.

Normal cash is issued by the government, but digital cash does not need to be. It could be denominated in market-determined, non-political monetary units.

Such a transition to a privately-operated digital cash system would require a period of brand-name recognition and long-term trust. Opportunities would abound for almost anyone, but in reality the greatest advantage currently goes to the on-line shopping malls and the large merchant sites on the Internet, such as Open Market, Internet Shopping Network, and Net Market. For it is this group that will directly influence the payment channel between consumer and merchant through their extensive contact with both. And, this influence could be used to their advantage to build preference for their "site" through money issuance in much the same way that various forms or coupons build customer loyalty and guarantee repeat visits.

Other potential unit providers include Internet service providers, bulletin board system operators, content publishers, card-based payment networks, and well-known manufacturer or service companies. They all share in common the existence of an extensive base of on-line customers. As the new digital cash providers, international brand names, such as Coca-Cola, Microsoft, and IBM, find themselves in an enviable position to capitalize immediately on their global name recognition.

6 Implementations of E-Money Systems

6.1 Introduction

In this chapter, we will investigate the different Digital Money systems known today. More specifically, we will look first at the desired properties of each system. Then we will take a look at the algorithms used. If the system is already in use, we will check the consequences of the introduction and the future plans of the company behind the system. Finally, we will present a critique of the system from different points of view.

6.2 Ecash

Desired Properties and Design Goals

Ecash was introduced by David Chaum [Cha85, CFN88, Cha92] and his company DigiCash [Dig95a]. The goal of ecash was to provide an anonymous, on-line digital money scheme that was easy to implement and to use.

Implementation

RSA (public key) cryptography is the basis of the ecash security. When executed for the first time, the ecash software automatically generates a pair of RSA encryption keys. Every person or entity using ecash has a unique pair of keys. One key will be kept secret (the secret key) and the other key will be made public (the public key). A party that wants to authenticate a message encrypts it with his or her own secret key: everyone can verify that the party signed this message by decoding it with the party's public key. A party that wants to send a confidential message, encrypts the message with the public key of the receiver: the receiver is the only one who will be able to decode the message.

Every person using ecash has an ecash account at a digital bank on the Internet. Using that account people can withdraw and deposit ecash. Ecash is a coin based system, which means that digital money is implemented by digital signatures that represent a certain fixed amount of money. We call such a digital signature a coin.

When an ecash withdrawal is made, the PC of the ecash user calculates how many digital coins of what denominations are needed to withdraw the requested amount. Next random serial numbers for those coins will be generated and a blinding factor will be included, to ensure anonymity. The result of these calculations will be sent to the digital bank.

The bank will encode the blinded numbers with its secret key (digital signature), and at the same time debit the account of the client for the same amount. The authenticated coins are sent back to the user and finally the user will take out the blinding factor that he introduced earlier. The serial numbers plus their signatures are now digital coins, their value is guaranteed by the bank.

The coins can be stored locally on the PC of the user. As soon as he wants to make a payment, his PC collects the coins needed to reach the requested total value. These coins are sent to the receiver, then the receiver sends them directly to the digital bank. The bank verifies the validity of these coins and that they have not been spent before. The account of the receiver is credited. Every coin is used only once. Another withdrawal is needed if the receiver wishes to have new coins to spend.

When using ecash, cash flows to its destination over the Internet (or any other computer network). The open architecture of the Internet requires security measures to be taken against attempts by a third party to intercept the digital money. Ecash provides high security by applying public key digital signature techniques. Additional security features of ecash include the protection of ecash withdrawals from the account with a password that is only known to the customer and not even to the bank.

One of the unique features of ecash is payer anonymity. When paying with ecash the identity of the payer is not revealed automatically. This way the payer stays in control of information about himself. During a payment a payer can of course identify himself, but only when he chooses so. Ecash offers one-sided anonymity, when clearing a transaction the payer is identified by the bank.

Today's Use

Today, almost 30.000 people are using ecash in the world wide trial. The digital money used in the trial, the Cyberbuck, can not be exchanged for real money, but valuable goods and services can be purchased in more than one hundred shops that have joined the trial and accept ecash cyberbucks.

The trial, which started in October 1994 and was closed for new testers a year later, introduced cash in cyberspace and created an enormous amount of interest from users, shops and banks as well as the media.

Already today, the Mark Twain Bank is issuing ecash denominated in US dollars and there are more to follow. DigiCash has adopted a non-exclusive licensing policy where DigiCash is the technology supplier. DigiCash is not going to offer ecash as a real money payment mechanism to individual users on the Internet by itself, because DigiCash is not a bank.

Future Plans

Although DigiCash is running an ecash bank in the trial, they do not intend to start an exchange between Cyberbucks and other currencies. A growing number of banks, financial institutions and other organizations are interested in issuing ecash, several ecash licenses have been sold. DigiCash currently follows a non-exclusive licensing policy, allowing multiple parties to issue ecash with their own, competitive, pricing structure.

Until this moment, ecash does not yet support Off-line capabilities or divisible coins. In [CFN88], David Chaum presented ideas to have Off-line capable coins and divisible electronic money. We can expect in the future that ecash will be extended to implement these properties as well.

Critique

Ecash is at the moment the only payment scheme which is truly anonymous. With David Chaum as one of the leading cryptographic experts, DigiCash provides a very solid basis for a secure and reliable implementation of digital cash.

6.3 CyberCash

Desired Properties and Design Goals

CyberCash was introduced in April 1995 in the US. It is providing a secure credit card transaction scheme for the Internet. A user must already possess a credit card.

CyberCash provides the interface between the credit card company, the merchant and the user.

Implementation

The CyberCash Wallet (CC Wallet) software enables the user to make instantaneous sales transactions with any CyberCash affiliated merchant. All transactions are encrypted to insure safety and privacy, by using 768-bit long RSA keys for key exchange and digital signatures and 56-bit DES encryption of messages. All transactions are authenticated with MD5 and 768-bit RSA signatures.

Today's Use

By installing the CyberCash Wallet software on a PC or Mac, the user will be able to make direct payments for goods and services over the World Wide Web and the Internet. Also, in the near future, on-line services will offer CyberCash secure payment services.

This version makes it possible to pay for goods and services with credit cards over the Internet by interacting directly with Web browsers. With CC Wallet, it is possible to create an account known as a "Wallet ID" which will be maintained by CyberCash Servers. Later versions will facilitate debit card, cash, and micro-payments as well.

CyberCash provides secure credit card transactions over the Internet since April 1995. It is processing thousands of transactions daily and is connected to 80% of the banks in the U.S. Over 400,000 CyberCash Wallets are today in distribution (includes CyberCash, Checkfree, and Compuserve).

Future Plans

In the future, CyberCash wants to enter the digital money market as well, using their own implementation of digital cash. Unfortunately, the algorithms and other details are not known today (Spring '96).

Critique

The advantage of CyberCash is that the system is similar to credit card payments which are well understood by the public. In the US, almost everybody has a credit card. It is therefore evident, why many people feel comfortable using this payment scheme. RSA and DES encryption already exist well over 10 years and are proven to be secure.

One concern about CyberCash is anonymity. All payments become traceable, as the system is based on credit card transactions.

6.4 NetBill

Desired Properties and Design Goals

NetBill was developed at Carnegie Mellon University by Doug Tygar and Marvin Sirbu. NetBill offers an electronic payment scheme for buying goods and services securely over the Internet. The transaction protocol is especially designed to handle low cost items, e. g. journal articles at 10 cents a page.

The protocol also ensures that both the consumer and merchant are protected: the consumer is guaranteed of the certified delivery of goods before payment is processed, and the merchant is guaranteed that the consumer cannot access the goods until payment has been received. This is achieved by delivering the goods to the consumer in encypted form, and only sending him the decyption key after payment.

NetBill acts as a third party to provide authentication, account management, transaction processing, billing, and reporting services for network-based clients and users. With a NetBill account and client software, users can buy information, software, CPU cycles, or other services from NetBill-authorized service providers, under a variety of payment schemes. NetBill acts like an electronic debit card service to provide financial services in support of electronic commerce.

Today's Use

NetBill was still in development during the writing of this writing.

Future Plans

Together with VISA, NetBill plans to become the payment scheme for small value transactions on the Internet.

Critique

Especially designed for low-cost items, NetBill provides a very innovative new idea, i.e to encrypt the electronic goods at the delivery, which the customer is going to decrypt after payment. Unfortunately, this scheme is not anonymous, as it relies on credit card transactions.

6.5 First Virtual

Desired Properties and Design Goals

FIRST VIRTUAL (FV) uses a very different approach to digital money. No encryption techniques are used. FV writes [Vir95]:

> With FV, encryption isn't needed. Encryption is almost always cumbersome and difficult. And it always adds an additional step, and something else to worry about. Rather than use encryption, we decided to design a system in which it wouldn't be necessary.

> By putting these insights together, the founders of FV invented a scheme that's so simple that everyone can understand and use it, yet robust enough that it can be used for almost any kind of information purchase. It's a system that lets most buyers try before they buy, and lets sellers set their own prices according to the return they require on their development costs.

FV intended to enter the electronic commerce market immediately, by using a simple system which is easy to implement. There are a few assumptions that FV assumes but did not state:

- E-mail is safe and can not be intercepted or forged by any impostor[9].
- E-mail travels fast over the network.
- If the buyer is satisfied with the information, s/he will be willing to pay the price for it.

Implementation

Transactions are all handled with a unique FV account identifier, which may safely travel in ordinary Internet E-mail. Even if it were intercepted, an unauthorized user couldn't use it for fraud. He or she couldn't even use it to buy information over the Internet fraudulently, because all transactions are confirmed via E-mail before they are charged. If someone tried to use a FV account identifier to buy something without authorization, the user will have to notify FV when he received the E-mail asking to confirm the charge, and the stolen account identifier would be deactivated immediately.

This system should allow the user to try before you buy. Under the FV scheme, if a buyer comes across something that looks interesting, he or she simply asks for a copy of the information, providing his or her FV account identifier to the seller. The seller then forwards information about the transaction, including the buyer's FV account identifier, to FV's Internet Payment System server.

FV's server then sends electronic mail to the buyer asking if the information was satisfactory. If the buyer decides that the information is of value, he or she replies "yes," and payment for the item is automatically transferred from the buyer to the seller. If the buyer decides the information is not worth keeping, he or she replies "no," and is not obligated to pay.

From time to time, buyers' credit card accounts are billed for the charges that have accrued during the billing period, and sellers' checking accounts are credited with payment for items sold. First Virtual handles accounting for both buyers and sellers.

Today's Use

FIRST VIRTUAL Holdings (FV) Incorporated is the world's first electronic merchant banker – a financial services company created specifically to enable the global buying

[9] It is not difficult for malicious hackers to intercept and forge E-mails.

and selling of information by anyone with access to the Internet.

FV began operations in May 1994. After months of testing, it officially introduced the FV Internet Payment System and technology at industry conferences and through the Internet in October 1994.

Today, several cybershops accept FV payments and people seem to use this system.

Future Plans

It does not look like FV will try to improve their system and add security in the future. FV claims that the system is safe and secure and therefore, no changes need to be made. Extending the market position seems to be the dominant future plan.

Critique

FV does not provide digital money. But it was the first Internet payment method. The problem with this scheme is clearly the lack of encryption methods. Internet E-mail is not safe at all and easy to forge. Building a payment system on such a weak basis without any cryptographic methods does not inspire confidence. Because most of the people do not know about cryptography, they can only believe FV's PR, which broadcasts the high security message. FV is also not anonymous at all. The scheme is built on the traditional credit card model, which makes every transaction traceable. Moreover, the messages are not encrypted and are vulnerable against a network eavesdropper.

There is one more big problem with the FV scheme: the buyer first receives the goods and then decides whether s/he wants to pay for them or not. In many cases, we can imagine that the buyer is not completely satisfied with the goods received, and will therefore not be willing to pay the entire sum. These kind of problems are usually very difficult so solve and require human interaction.

6.6 Mondex

Desired Properties and Design Goals

In England, another digital money scheme emerged: Mondex. Cryptographic methods were used, but none of the methods is published. Unfortunately, this does not raise trust into the system.

Mondex has been designed to be a global payment system. International interoperability has been catered for by the adoption of standards, in the selection of the Mondex Brand and the employment of language-independent ergonomics. This means that it should be as easy to use a Mondex card in a shop in the UK as it will be to do so in Japan or India.

Implementation

Instead of carrying notes and coins, Mondex consumers will carry a Mondex Card, on which cash is stored electronically. Cardholders can load money onto their cards at a new generation of cash dispensers, payphones and homephones.

Mondex also enables person-to-person payments. Using a Mondex wallet, two cardholders can transfer cash between their cards. With a Mondex telephone, person-to-person payments can be made across the world. In everyday use Mondex transactions are private, just like cash.

However, if the card is lost, a unique 16-digit identity number stored on the chip, which will have been registered by a card-providing bank against the personal details of the customer, may be used in order to return the card to its rightful owner.

Mondex is open and has no requirement for on-line clearing – it is a payment system with the potential to be accepted everywhere. It has been developed as an alternative to traditional cash by allowing value to be received and transmitted between parties who are unrelated other than through their participation in the scheme, without the involvement of a third party.

Today's Use

NatWest has joined forces with Midland Bank to purchase the Mondex franchise in the UK. The two banks have established a joint venture company, called Mondex UK Limited. Together with BT, the banks will be responsible for the pilot being undertaken in Swindon and eventual national rollout of Mondex. On 3 July 1995, MONDEX was launched in Swindon.

A high-street newspaper vendor in the UK made history when he officially became the first person to exchange goods for electronic cash in the UK.

Don Stanley, 72, parted with a 28p newspaper in return for "cash" stored in the microchip in his customer's Mondex card.

The simple transaction marked day one of a pilot in Swindon, Wiltshire, the first step in the introduction of a global alternative to cash. From now on, Swindon's shoppers will be able to pay for goods and services at outlets – from corner shops to department stores – without having to worry about breaking into 20 pound notes or fiddling with small change.

Mondex is based on the electronic storage of money on a plastic smart card. It can be used to pay for goods and services in the same way as notes and coins, and the "cash" can be transferred from one card to another, or to and from a bank account, using a range of Mondex devices or compatible BT phones.

Unlike transactions using credit or debit cards, Mondex transactions do not involve authorization or signatures and there is no chance of incurring debt because users can spend only what is available on their card.

The Swindon pilot is set to last up to two years and is expected to involve up to 40,000 consumers and 1000 retailers.

Mondex UK Chairman, Tony Surridge, said: "We're updating a form of payment which has been around for thousands of years. And while Mondex is essentially the same as cash, we've been able to add in a few important improvements – such as being able to send or receive money down a phone line."

Ken Howes, Head of Group Card Development at Midland Bank, said: "Although we expect the Swindon pilot to herald a 'less-cash' rather than a 'cashless' society, we believe that people will find Mondex extremely convenient and will use it as they use cash now."

Future Plans

Beyond the pilot, Mondex will be extended across the UK and internationally. The Bank of Scotland has already agreed to participate in the scheme on a national level, the Hong Kong and Shanghai Banking Corporation Limited has purchased the rights to Mondex in the Far East and the Royal Bank of Canada and Canadian Imperial Bank of Commerce have purchased the rights to Mondex in Canada.

Critique

Unfortunately, Mondex does not publish unbiased reviews about the Swindon pilot. We can imagine that there were also critical voices, but none were published by Mondex. Especially the secrecy of the algorithms does not inspire confidence for this system.

There is a paradox left: On one side, Mondex is completely off-line capable, but at the same time anonymous. Let's imagine a scenario with the three characters Alice, Bob and Carol. Alice has possession of a valid bill X and gives it to Bob in return for some goods. Now both Alice and Bob buy goods from Carol and both pay with the same bill X. The question now for Carol and the bank is: Who duplicated the bill, was it Alice or Bob? Because of anonymity, we can not know. Maybe Mondex solved this problem described in the above scenario. But making their implementation secret, we can question the quality of the information released by Mondex[10].

In fact, a British agency in charge of consumer protection has begun a formal investigation of Mondex for allegedly falsely advertising that transactions under its system were anonymous.

In promotional materials, Mondex had claimed that the transactions were "just like cash." In reality, each card used in the system has a 16 digit identifying number which is captured by the merchant and transmitted to the bank each day. The merchants readers can retain up to 500 records at one time. Mondex's Swindon manager admitted in Network Week, a trade publication, that "we can certainly trace where cards have been used."

The investigation began after Simon Davies, a Law Fellow at the University of Essex and Director General of Privacy International, filed a complaint.

[10] Mondex did not describe the problem in their documentation and did therefore not state to have solved it either.

7 Advantages of Digital Money

7.1 For Users

One of the benefits for the user is increased convenience. Just think of road toll payments that can be made from moving vehicles. No more bulky cash to carry around, no worrying about change.

Increased convenience also derives from the freedom of individuals to obtain their card computers from any source, to use whatever hardware or software they choose, and to interface with communication systems wherever they please. This permits card computers to be adapted to the requirements of sophisticated, naive, and handicapped users alike. Most ATM machines nowadays can not be accessed by handicapped people, and even other people refuse to use ATM machines due to various reasons. Some of them think they are too complicated to use or they can't remember their personal identification number, and others just don't like to interact with a machine. They prefer to talk to a human being.

Using digital cash, people might choose never to actually see their digital pseudonyms or to be concerned with other implementation details.

The user is also protected against the bank's refusal to honor a legitimate note, since nobody is able to counterfeit the bank's digital signature on the note.

An other important benefit for the user is improved security. By requiring a password akin to the PIN (personal identification number) now used for bank cards, the electronic wallet could safeguard itself from abuse by thieves by making encrypted backup copies of its contents. A replacement card could then recover these contents if the original electronic wallet were lost.

At the same time, abuse of a lost or stolen card computer by another individual would be very difficult without the owner's secret authorizing number. The card would require the authorizing number, which might typically be about six digits long, before allowing any transactions. A reasonably tamper-resistant device within the card computer could for example

- read fingerprints or the like to prevent use by anyone but the card owner
- accept a special authorizing number that the owner could use in case of duress to trigger a prearranged protective strategy
- permit only the current owner to reset the card for a new owner, to prevent its use as a replacement by a thief

True anonymous digital cash[11] would also provide unconditional untraceability. The "blinding" carried out by the user's own device makes it impossible for anyone to link payment to payer. But users can prove unequivocally that they did or did not make a particular payment, without revealing anything more, if they need to. And of course, the dangers deriving from computerized pattern recognition techniques mentioned earlier would be non existent.

[11] like the one provided by DigiCash

7.2 For Banks

Digital cash offers reduction in cost for banks in several ways.

First of all, processing effort might be lower than with existing post-pay cards since single transactions need not be authorized on line, debited from the customer's account or printed for the customer. This will be particularly true for small amounts of payment.

Furthermore, the current card system requires widely trusted, tamper-resistant devices at all points of entry to transaction systems. Such a requirement implies substantial initial agreement, outlay, and commitment to design, and can be expected to result in technology that is outdated when systems come into widespread use.

With the security measures built into the electronic wallet mentioned above, fraud costs and costs for clarifying disputed transactions could be reduced. Nowadays, card fraud is a very important problem.[12] The same argument applies also to card counterfeiting and forged bank notes.

Other costs linked to normal cash are costs for printing and mailing statements to customers, or the costs for handling cash and for cash dispensers. These could be reduced with home banking possibilities, i.e. transactions that can be made using your personal computer at home.

If the digital cash system implemented were anonymous, it would also reduce the sensitivity and the quantity of consumer data in the hands of the bank and by the same token, it reduces their exposure to incidents that might incur legal liability or hurt their public images.

7.3 For the Issuer

There would be no more need to find new security techniques to print bank notes. Printing costs would also disappear.

Another aspect is also that the system provider does not need to supply user organizations with tamper-resistant terminal equipment for each entry point, any more than he needs to supply card computers to individuals. Thus, user organizations can supply their own terminal equipment wherever they please and take advantage of the latest technology.

7.4 For the Retailers

First of all, stored value payments should be a lot faster than post-pay payments. Infrared payments might also be faster than cash payments, resulting in a saving of time.

But costs could also be reduced. Nowadays, retailers must pay a fee of 2 to 7 percent of the purchased amount to the credit card company. The fees for digital cash transactions are likely to be smaller than for today's cards because of smaller operating costs for the issuer.

[12] In 1993, card fraud cost English banks about 130 million pounds [WCP+95].

There would also be less vandalism, since with infrared interfaces, there are no slots or contacts. Ticket vending machines could use electronic receipts rather than printers. This would reduce maintenance costs.

In general, infrared terminals should be cheaper than stripe or chip card terminals and won't wear off as fast.

Vending machines would not need tamper resistant modules except if aggregating totals.

Of course back office costs for counting, storing and transporting cash would fall away.

8 Disadvantages of Digital Money

8.1 Global Disadvantages

Safety is the major problem of all the payment systems seen above.

What if the chosen cryptographic algorithm is not safe? Most algorithms used in these monetary systems have been around for many years already (DES [DP92], RSA [RSA78]), and some of the best cryptology experts tried to break them using sophisticated methods without success. Although one can never exclude the possibility that someone invents a new brilliant way to attack a given algorithm, chances that this might happen are still very small.

Another weak spot is the users personal hardware (e.g. the electronic wallet) and his copy of the software. Only complete physical security can guarantee that nobody can ease a user of some money.

The installation in the bank must be perfectly secure too. Just imagine the following:

In the system that DigiCash uses, digital notes can be identified by verifying the bank's signature on the note. The bank's signature can not be forged, since the bank is the only one that knows the secret key. Imagine what would happen if someone outside the bank would get hold of that secret key. He then would be able to create an unlimited amount of money, thus threatening to collapse the market. Or what if terrorists drop a bomb on the one central bank building that holds the secret key? A new key would have to be generated and all digital "coins" using the old key would have to be exchanged. A solution to that problem would be to make copies of the secret key and store them in different locations, but if several copies of the key exist, the risk that someone can get hold of one gets higher.

Another disadvantage is a possible uncontrolled growth of E-cash systems. Such a monetary explosion could undermine bank- and government-controlled money systems, giving rise to a confusing and inefficient Babel of competing systems.

8.2 For Users

The disadvantages presented in this subsection might seem not very weighty, but on second sight they are at least of the same importance than the other disadvantages mentioned before.

First of all, fewer people can understand the technology behind digital money, and thus it does not inspire confidence. Conventional money on the other hand does not require any profound knowledge in order to use it.

The rising of E-cash could also foster a have and have-not society: Those with PCs would have ready access to the new technology, while those without, many of them low-income consumers, would not.

With digital cash, numbers stored somewhere in a pocket computer, the notion of money is somewhat lost. Sometimes we use the physical tangibility of cash in order to hand money personally to someone else, e.g. as a gift, as charity, or as a tip. This cannot be done with digital cash. With regard to tips, it is important for waiters, for example, to have some means to supplement low pay. It is not certain that procedures such as rounding up the bill, or leaving some coins on the table will occur when digital cash is used.

Also, children might have difficulties to learn to get a feeling of "how much" something costs. Handhold readers that display balances might be of help, but will probably not be fully equivalent to the look and feel or the symbolic meaning of cash.

8.3 Legal problems

It will be a lot harder for the government to control E-cash than real cash. Money laundering and tax evasion could proliferate in stateless E-money systems. If the monetary system were anonymous, criminals could use untraceable cyberdollars to hide assets offshore.

That is why the American government is trying to make the public key/private key system that is used by DigiCash and others illegal. The government would prefer for everyone to use their Clipper chip, which is similar to the above method, except that they can also tap in "if necessary".

In France cryptography is completely forbidden by the law. Obviously this is currently an area of heated debate.

9 Conclusion

In this report we tried to compare the different electronic commerce schemes and their impact on society. After a careful study of the various implementations and systems, we must state the following observations:

- Because considerable sums of money are involved in the electronic money market, some companies prefer to enter the market as quickly as possible, even with a mediocre system.
- The consumer is not well enough informed on all the risks involved. The inherent complexity of the domain forbids the greatest part of the population to see the threats and risk on their own.
- The risk of a possible disclosure of the bank's private key was not addressed in any of the documents we read. The publication of the secret keys would

have catastrophic impacts on the society, as everybody would then be capable of producing money.

- An introduction of digital cash in a large scale will certainly alter the way people handle money, but may also trigger fundamental changes in modern society.

These elements show that we must be very careful when choosing or implementing an electronic money scheme. Many of the risks involved are not clear to the common user. Further, the amount of money involved makes it profitable to criminals to invest considerable amounts of money to break the system.

Digital money, a divine gift or Satan's malicious tool? Keeping the exponential growth of the Internet in mind, it is clear that we will need an electronic payment scheme in the near future. It is everybody's responsibility to face the critical issues and decide for a reliable and secure system. The coming years will show whether or not this responsibility was recognized and all of the problems have been solved by the creators of the digital money.

10 Acknowledgements

First of all, we would like to thank Dominique Joye for his suggestions and helpful discussions throughout the writing. Our thanks also go to Michael Waidner of the IBM Security Research Group and Arnd Weber from the Special Interest Group for Multicurrency Electronic Wallets, who helped us to find social related information by sending us the CAFE report containing digital money related surveys conducted throughout Europe. Discussions with Uwe Wilhelm of the LSL at EPFL were also stimulating. Special thanks to Sonja Nießen for proof-reading the document.

References

[Ban95] David Bank. Digital dollars. WWW at Mercury Cernter web, January 1995.

[BB93] E. Bach and S. Bellovin. Cryptography faq. WWW, August 1993.

[Bra88] Gilles Brassard. *Modern Cryptology, A Tutorial*, volume 325 of *LNCS*. Springer, 1988.

[CFN88] David Chaum, Amos Fiat, and Moni Naor. Untraceable electronic cash. In *Advances in Cryptology - CRYPTO '88*, volume 403 of *LNCS*, pages 319 – 327. Springer Verlag, 1988.

[Cha85] David Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10), October 1985.

[Cha92] David Chaum. Achieving electronic privacy. *Scientific American*, pages 96 – 101, August 1992.

[CLR90] Cormen, Leiserson, and Rivest. *Algorithms*. MIT Press, 1990.

[Cyb95] CyberCash. WWW at http://www.cybercash.com, 1995.

[Dam88] I. Damgard. Payment systems and credential mechanisms with provable security against abuse by individuals. In *Advances in Cryptology - CRYPTO '88*, volume 403 of *LNCS*, pages 21 – 25. Springer Verlag, 1988.

[Dig] Digicash. Digicash - numbers that are money. WWW at http://www.digicash.com.

[Dig95a] DigiCash. WWW at http://www.digicash.com, December 1995.

[Dig95b] Digicash. Digital signatures and smart cards. WWW at http://www.digicash.com, 1995.

[Din95] Andrew Dinsdale. Cyber cash, the secure internet payment service. WWW, 1995.

[DP92] D. W. Davies and W. L. Price. *Security for Computer Networks*. John Wiley and Sons, LTD, 1992.

[Knu81] Donald E. Knuth. *The art of Computer Programming*, volume 2 Seminumerical Algorithms. Addison Wesley, 1981.

[KWS96] Jörg Kienzle, Thomas Wolf, and Alfred Strohmeier. Secure communication in distributed ada. In *Still in Preparation*, volume not yet known of *LNCS*. Springer Verlag, 1996.

[Lem] Judith Lemon. Electronic commerce: the critical issues. WWW. An Interview with Marty Tenenbaum and Allan Schiffman of Enterprise Integration Technologies.

[Lev95] David Levy. E-money (that's what i want). *Wired http://www.hotwired.com*, 1995.

[LMP94] Steven H. Low, Nicholas F. Maxemchuk, and Sanjoy Paul. Anonymous credit cards and its collusion analysis. Technical report, ATT Bell Laboratories, Murray Hill, NJ 07974, October 1994.

[Mat95] Jon W. Matonis. Digital cash and monetary freedom. WWW at http://www.nttam.com, May 1995.

[Mon95] Mondex. WWW at http://www.mondex.com, 1995.

[Orw48] George Orwell. *Nineteen eighty-four*. Penguin Books, 1948.

[PWP87] Birgit Pfitzmann, Michael Waidner, and Andreas Pfitzmann. Rechtssicherheit trotz anonymitaet in offenen digitalen systemen. *Computer und Recht*, 12(3/10), 1987.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method of obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.

[SUN95] SUN. *Cryptography in Public Internetworks with SunScreen*, May 1995.

[Vir95] First Virtual. WWW at http://www.fv.com, 1995.

[WCP+95] A. Weber, B. Carter, B. Pfitzmann, M. Schunter, C. Stanford, and M. Waidner. Secure international payment and information transfer. Technical report, CAFE Project, 1995.

[Ylo] Tatu Ylonen. Introduction to cryptography. WWW.