
# Internet Security and Privacy

## Digital Cash

**Batch: 2005-2006**

Submitted By: Charu Gupta – char-gup@dsv.su.se
Stalin Subramaniam – stalins@kth.se

# Introduction

Exchange mechanism has long been used and evolved through time. Starting from the barter system to the modern way of trading it is clear that the need of an imperative commodity to serve this exchange procedure is essential.

With the growing popularity of Internet usage the digital cash or electronic money is taking the world by storm. It is one of the modern methods of exchange where users are dealing with technology to complete and exchange process rather than dealing with it manually. The digital money is nothing but the money represented by computer files. It refers to the conversion of the money into the binary form of the computer data. This money works like real cash except that it is not in a form of paper like real currency notes. It is rather in the form of a smart card or computer network money. The digital money has just a computer chip which is capable of storing a huge amount of information. Typically, this involves the use of computer networks such as the Internet and digital stored value system. The basic scenario is:

- The customer opens an account in the bank in a usual manner.
- When he needs the electronic money he sends a mail to the bank which is encrypted sending his request.
- The bank authenticates the message and when sure debits the customer's account with the amount asked for.
- The bank sends the money as a computer file which contains an extremely huge amount of random number to the customer in an encrypted form.
- Now the customer wants to make a purchase using this money. He sends the necessary file to the person from whom he wants to make a purchase in an encrypted form.
- The recipient sends the file to the bank which verifies it and credits his account with the actual money equivalent to the value of the electronic money.

This is how basically the digital money works. The certain qualities desired to be fulfilled by digital cash are

### *Qualities Desired*

- ***Security:*** The first and foremost desirable quality of digital cash is that it should not be copied, reused and should be able to clear all the authentication levels like user identification, message authenticity and non repudiation.
- ***Privacy:*** Another quality expected to be fulfilled is that it should be able to maintain the privacy of the person i.e. the transactions carried out through this money should not be traceable.
- ***Portability***: It should be free from the dependence on any physical location.
- ***Transferability:*** The user should be able to spend the money as he likes without having to contact the bank every time.
- ***Divisibility:*** The note should have the capability of being subdivided into smaller pieces of cash i.e. the customer should be able to spend only a part of the money and have the remaining money with him if he wants.
- ***User Friendly:*** It should be easy to use by both the customer giving it for buying goods and the merchant getting it.

These are the certain qualities which are expected to be fulfilled by the digital money and the various digital cash protocols.

# Digital cash Protocols

### *Protocol 1: Identified Digital Cash*

This works a lot like a credit card. The progress of the electronic money from the very first time it is issued by the bank to the customer to its final return to the bank is as follows:

- The customer sends the request of digital money to the bank.
- The bank authenticates the request and on confirmation generates the serial number and sends it along with the electronic money to the customer.
- The customer spends the money and the merchant from whom he made the purchase has the money now.
- To encash the money the merchant sends it to the bank.

However this protocol does not protect the privacy of the person carrying out the transaction as the money has the same serial number therefore the bank knows that the customer has bought something from which person and on what date. This problem could be solved by using anonymous electronic money protocol.

### *Protocol 2: Anonymous Electronic Money*

In anonymous or blinded protocol there is no trail of the transactions involved. The protocol works as follows:

- The customer prepares 100 bank notes.
- Each say the value of the note (how much money does that note represent) and has a long random number.
- He puts each one of them in a different envelope with a carbon paper and seals the entire envelopes and sends them to the bank.
- The bank opens all the envelopes except one.
- If all the notes are for the same amount, the bank signs the blinded note (the unopened envelope) and deducts the amount from the customer's account and sends the signed note to him.
- When the customer receives the note he un-blinds(opens the sealed envelope) it.
- He carries the business with the merchant. The merchant checks the signature and sends the random number to the bank.
- If the bank says they have not seen this random number, the vendor accepts the note.

This protocol protects the identity of the customer because the bank signed the blind note and does not know about the serial number. The customer has only one percent chance of cheating as the bank can open any of the envelopes for verification. However this protocol does not satisfy the quality of security as the customer can copy his note after the bank signs it and use it twice. This is known as double spending problem. This can be improved by slightly modifying the above protocol. After the business the merchant brings the note to the bank and the bank on verifying the legitimacy of the note credits the merchants account and stores the number of the note in its database. Now the customer

cannot cheat as if he copies the note and tries to spend it twice, the bank would come to know of it from its database and will not accept the note.

However this protocol requires the merchant to contact the bank at every transaction to ensure that the customer is not trying to cash the note twice. The bank has to actively participate in the transaction between the merchant and the customer. So this is also known as **online electronic money**. This compromises on the quality of user friendliness and we can prevent the active participation of the bank during the transaction using the ***offline e-money protocol*** which works as follows

- The customer prepares 100 bank notes.
- Each say the value of the note and have a long random number. The notes also contain pairs of identity bit strings which contains information about the customer like his name, address and the other identifying information about him .Then the customer splits the information into two pieces using secret splitting protocol and commits to each piece using bit commitment protocol.
- The customer blinds all the notes and sends them to the bank.
- The bank asks the customer to un-blind all the notes except for one. The bank also asks the customer to reveal all of the identity strings.
- The bank verifies that the customer is not trying to cheat and on being sure that the customer is not trying to cheat ,the bank signs the note and deducts the amount from his account and sends the signed note to him.
- To spend the note, Alice gives the note to a merchant.
- The merchant first checks the banks signature on the note. If the signature is correct he proceeds. He asks the customer to randomly reveal either the left half or the right half of the identity string and the customer does it.
- At some point in the future, the merchant submits the note to the bank. The bank verifies the signature by checking the entries in its database. If it is present, the bank compares the identity string of the money order with the one stored in its database. If it is same the bank knows that the merchant is trying to cheat by copying the note

and if it is different it knows that the customer is trying to cheat. If the uniqueness string is not present in the database the bank credits the amount of the merchant.

This protocol can give rise to double spending problem. The customer could spend it offline more than once in quick succession with two different merchants. Since the bank is not involved in the transaction the customer could easily cheat. But since the merchant to whom the customer gives the money order the second time will have the different selector string than the first merchant because half the time the two merchants ask for different values to be revealed. The bank XOR's the two values and comes to know the identity of the customer.

# The Various models

### *1. Electronic Purse Model*

In this model we make use of smart card which contains the electronic information about the notes instead of real notes but will work as real cash. Smart card has a small electronic chip which can be used to store huge amount of information. Here the information about the card is sent in an encrypted form to prevent eavesdropping and after the transaction the bank deducts some amount of money from customer's account and it credits the seller's account with the same amount as it had debited from the Customer's account using the payment protocol. The electronic purse will reduce the hassle of carrying the paper notes and coins but will work exactly like real cash.

### *2 . The Cheque Model*

In this model Alice gets a specification file from Bob which identifies him and also contains information about time, a transaction number, payment terminal identity and Bob's acquiring bank. After verifying the files authenticity Alice adds more information like her identity, her purse identity and signs it with her private key. The digital signature of Alice is a proof that the transaction has been carried out successfully and the bank credits and debits Bob's and Alice's account respectively with the same amount of money that is believed to have been used in the transaction. The balance and the private key are to be kept safe and protected in this model. This model can be used in online mode where all transactions are verified by bank at that instance only or in offline mode using certificate.

So this model can be used both for anonymous electronic money protocol and offline electronic money protocol.

### *3. The Cash Model*

In this model the digital money is in form of pair of strings where first element is the serial number of the note and the other element is the digital signature of the bank verifying its issuance. This model is based on the offline electronic money protocol. Using this model the active participation of the bank would not be required and the persons carrying out the business can do it any time without verifying the authenticity of the note with bank every time. However the use of this model gives rise to double spending problem as discussed in the protocols. The Bank's signature is to be protected in this model.

# Challenges of using digital cash Advantages and Disadvantages

### *Advantages*

The increasing usage of Internet has given use to applications like internet shopping etc where people can buy anything online using their credit cards. Unfortunately the transactions carried out using credit card are traceable and the bank knows exactly how much and where you have spent the money. It is the form of invasion to person's privacy. However the electronic money respects the privacy of people. The transactions carried out using this form of money lend anonymity to the person unless he cheats. Besides privacy it also provides security in carrying out online transactions which is always a risk in the case of credit cards.

Digital cash will allow for the immediate transfer of funds from an individual's personal account to a businesses account, without any actual paper transfer of money. This offers a great convenience to many people and businesses alike.

Banks can offer many services whereby a customer can transfer funds, purchase stocks, contribute to their retirement plans and offer a variety of other services without having to handle the physical cash or cheques. Customers do not have to wait in lines, and this provides a lower hassle environment.

***Disadvantages***

Although there are many benefits to digital cash, there are also many significant disadvantages. These include fraud, failure of technology, possible tracking of individuals and the loss of human interaction. It is very common that almost all systems have drawbacks. However the question that needs to be asked is whether the advantages of using the system overpass the disadvantages.

Fraud over digital cash has been a pressing issue in recent years. Hacking into bank accounts and the illegal retrieval of banking records has led to a widespread invasion of privacy, and has promoted identity theft.

There is also a pressing issue in regards to the technology involved in digital cash. Power failures, loss of records, undependable software often cause a major setback in promoting the technology.

Another problem that has made people reluctant to use the many advantages of digital cash is 'Baby Boomers' problem. In this suppose a baby is kidnapped and the kidnapper prepares the anonymous money order of the amount he wants, blinds them and send them to the bank with the threat of killing the baby if the demand is not met. The bank has to sign all the notes and publish the result in the newspaper. Now the kidnapper frees the baby and after buying the newspaper unblinds all the notes and spends them easily. This is a perfect crime and thus makes people wary of using digital cash.

# Conclusion

Nowadays the traditional bills and coins are giving way to the electronic money. With the wide spread of Internet this transformation is inevitable. It is obvious that digital cash is the future of exchange mechanism. It will surely condense many of the prevailing inconveniences such as carrying large amount of cash and will resolve many of the in-security issues experienced today. The electronic money would not only be quicker and cheaper but also more robust and easy to authenticate. People would not be apprehensive in using it as it will respect their privacy and will allow even small merchants to carry out the business all over the world. The digital cash will also reduce the cost of transferring the money internationally which is quite expensive at present. The electronic money will not replace the traditional form of transaction completely but will facilitate it surely.

# References and Bibliography


1. Applied Cryptography by Bruce Schneier
2. Network Security Essentials by William Stalling
3. http://www.ex.ac.uk/~RDavies/arian/emoneyfaq.html
4. http://www.sfasu.edu/finance/fincash.htm
5. http://www.simovits.com
6. http://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS4/DigitalCash.doc
7. http://www.virtualschool.edu/mon/ElectronicProperty/EconomicConseqDigiCash.html
8. http://en.wikipedia.org/wiki/Digital_cash

(All links retrieved on 20 November ,2005)