# Digital Cash

**By**

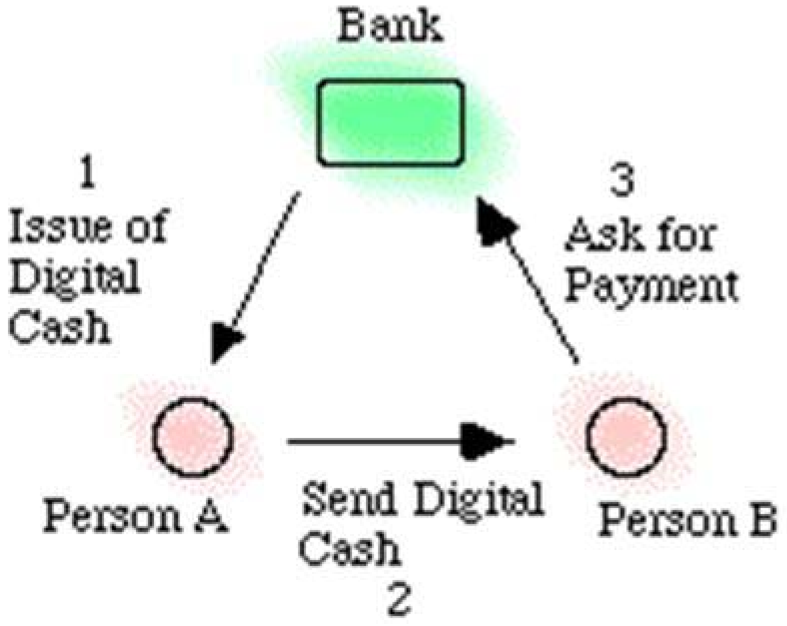
**Presentation Date: 26/2/2004**

**Team members: Amit, Hiren, Kevin, Kai**
**Supervisor: Stefano Cattani**

## What is Digital Cash?

Essentially, digital cash mimics the functionality of paper cash. More technically, digital cash is a payment message bearing a digital signature which functions as a medium of exchange or store of value. Paper currency and coins represent value because they are backed by a trusted third party, the government and the banking industry. Digital coins will also represent value because they are backed by a trusted third party, usually a bank that is willing to convert digital cash to physical cash.

## How does Digital Cash work?



There are a number of electronic cash protocols. To a degree, all digital cash schemes operate in the following manner: A user installs a "cyber wallet" onto computer. Money can be put in the wallet by deciding how much is needed and then sending an encrypted message to the bank asking for this amount to be deducted from the user's account. The bank reads the message with private key decryption and verifies if it has been digitally signed in order to identify the user. The bank then generates "serial numbers", encrypts the message, signs it with its digital signature and returns it. The user is now entitled to use the message (coin or token) to spend it at merchant sites. Merchants receive e-cash during a transaction and see that it has been authorized by a bank. They then contact the bank to make sure the coins have not been spent somewhere else, and the amount is credited to the merchant's account.

## Key Properties of a Private Digital Cash System

The use of digital cash is not dependent on any physical location, and can be transferred between the physical world and virtual world of the Internet Smart card integration with computer networks have been proposed to offer this functionality. Real cash is limited by its physical form .Cash represented by streams of 0's and 1's can take advantage of its electronic nature, and permeate through networks and digital sale devices at light-speed, worldwide.

**Ideal properties:**

**1. Secure.** The transaction protocol must ensure that a high-level security is maintained through sophisticated encryption techniques. For instance, Alice should be able to pass digital cash to Bob without either of them, or others, able to alter or reproduce the electronic token.

**2. Anonymous.** Anonymity assures the privacy of a transaction on multiple levels. Beyond encryption, this optional intractability 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. 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.

**3. Portable.** The security and use of the digital cash is not dependent on any physical location. The cash can be transferred through computer networks and off the computer network into other storage devices. Alice and Bob should be able to walk away with their digital cash and transport it for use within alternative delivery systems, including non-computer-network delivery channels. Digital wealth should not be restricted to a unique, proprietary computer network.

**4. Two-way.** The digital cash can be transferred 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. 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.

**5. Off-line capable.** 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. Alice can freely pass value to Bob at any time of day without requiring third-party authentication.

**6. Wide acceptability.** The digital cash is well-known and accepted in a large commercial zone. Primarily a brand issue, this feature implies recognition of and trust in the issuer. 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.

**7. User-friendly.** The digital cash should be simple to use from both the spending perspective and the receiving perspective. Simplicity leads to mass use and mass use leads to wide acceptability. Alice and Bob should not require an advanced degree in cryptography as the protocol machinations should be transparent to the immediate user.

## Categorization of Digital Cash

It is apparent that various authors have different specifications for e-cash. There are a number of categories in which these descriptions may be distinguished.

**1. Anonymous or Identified.** Anonymous e-cash works just like real paper cash. Once anonymous e-cash is withdrawn from an account, it can be spent or given away without leaving a transaction trail. This however, can be considered contentious, such as Paypal, a recognized form of digital cash, is not considered to be entirely anonymous.

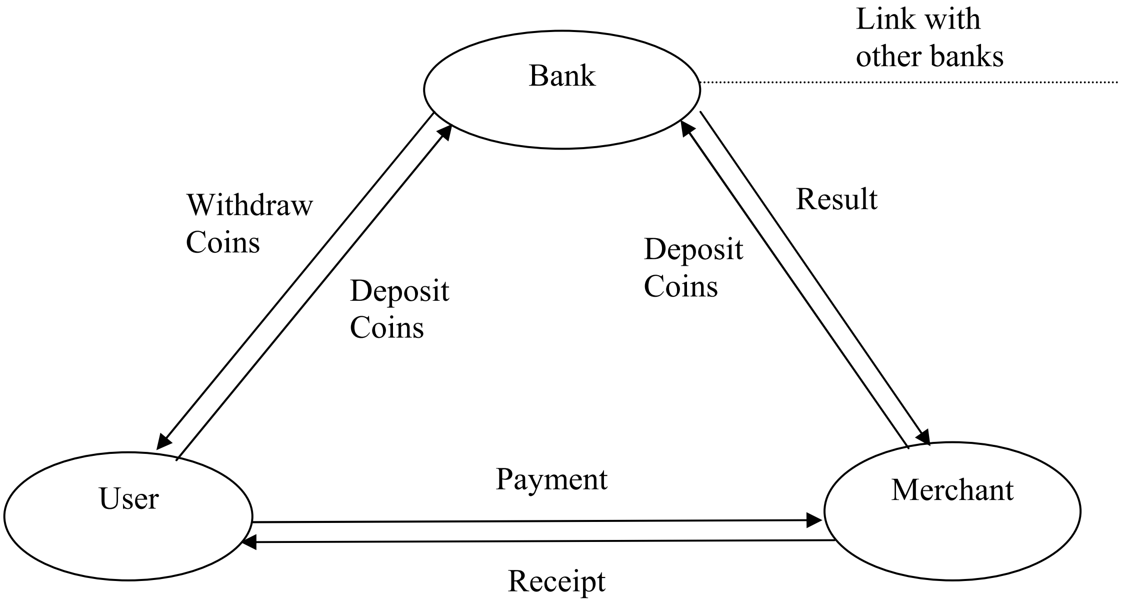
**2. Online or Offline.** Online means you need to interact with a bank (via modem or network) to conduct a transaction with a third party. Offline means you can conduct a transaction without having to directly involve a bank.

**3. Smart Cards or Purely Electronic.** Smart cards are similar to credit cards, but store money-related information on a chip within the card. They may be used in digital cash applications. Again, there is ambivalence as to whether smart cards represent "true" digital cash. Critics claim smart cards encumber peer-to-peer transactions and are not purely electronic as the digital cash protocols related to networks and the internet.

## General models for Digital Cash

As it was mentioned in the introduction, there are two types of system for digital cash, namely, the online system and offline system. In the following, systems' structure, advantages and disadvantages are discussed.

### Online Digital Cash



The diagram above shows the structure of the online digital cash system, the structure is indeed very similar to the one which is being used in the existing paper cash system. In this system, we have got three main components; the bank, customers and merchants, the user withdraw coins from the back, spend in the shop and the shop deposit the coin back to the bank.

The user ID in this online digital cash system is fully anonymous and it is done by using a protocol called Blind Signature Protocol. This protocol simply eliminates the association between the user ID and the serial number of the coin. Although it is good to hide user's identity totally, but this raises the problem of "double spending" – since the digital cash is digitally represented, it is very easy to duplicate and let the user spend the coin twice.

To tackle the double spending problem, the merchant has to verify the coin with the bank at the point of sale in each of the transaction, this verification of the legitimacy of the coin requires extra bandwidth and is a potential bottleneck of the system especially when the traffic is high. The real time verification also means there is a need for the synchronization between bank servers.

## Pros and Cons of the online digital cash system

Here is the summary of the pros and cons of the online system:

**Pros**

- Provides fully anonymous and untraceable digital cash:
  - Provides user with confident that their user ID will not be revealed in anyways.

- No double spending problems.
  - Double spending is not possible at all due to the fact that coins are checked in real time during the transaction.

- Don't require additional secure hardware
  - No additional hardware is needed for the implementation; existing POS (Point of Sale) devices could be used with a software update.

**Cons**

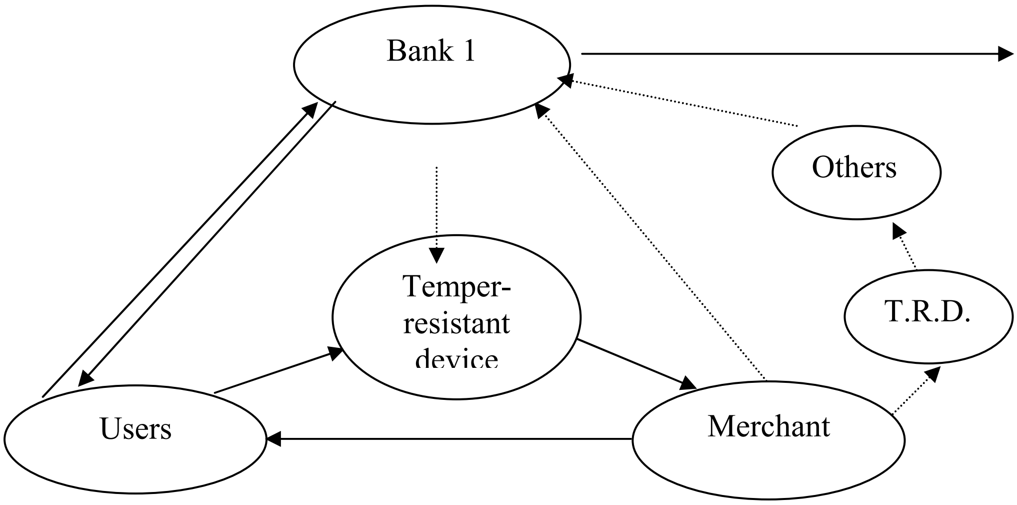
- Communications overhead between merchant and the bank.
  - The cost of the extra security and anonymity also becomes the bottleneck of the system due to real time verification.

- Huge database of coin records.
  - The bank server needs to maintain an ever-growing database for all the used coins’ serial numbers.

- Difficult to scale, need synchronization between bank servers.
  - There is a need to perform synchronization of coin’s serial numbers every time a coin is deposit into the bank. This is simply impractical.

- Coins are not reusable
  - It has to be deposited back to the bank for verification; therefore, coins can only be used once.

## 2. Offline Digital Cash



In the off-line scheme, the withdrawal and disposal of the coins are very similar to the one in the on-line scheme; the main difference is in the transaction part of the model. Instead of verifying coins during every transaction, the security of each entity in the system is guaranteed without a direct involvement with the bank. This is achieved by adding an additional component in the model called the "Temper – Resistant Device". In a real life example, you could think of it as the Smart Card Reader at the Point of Sale. The device is trusted by the bank and is used to verify the authenticity of the coin but does not check whether the coin has been double spent. This device makes the whole transaction offline but let the system suffers from the double spending problem. Therefore, we need a new method to let the bank to trace back who double spent the money but at the same time, keeping the system to be anonymous. One may ask that how could a system be traceable and anonymous? Are they not the opposite of each other in the first place? A method called "Secret Splitting" is commonly used to allow the user to be anonymous as long as he/she doesn't double spend. The technique will be explained later in this handout.

So now, having tackled the problem of double spending and making it offline, the merchant can deposit the collective amount of coins before it deposit back to the bank possibly at the end of the day. Notice that the system could be implemented so that the coin itself can be reusable. The merchant can spend the coin elsewhere with other parties through another temper-resistant device before the coin finally deposited back to the bank for verification.

In additional to the secret splitting method, in order to add extra security to the offline system, there could be a link between the bank and the temper-resistant device which allows the T.R.D. to download a blacklist of double spenders in a set period of time when the traffic is low. This reduces the chance of people double spending their money in the first place.

## Pros and Cons of the offline digital cash system

### Pros

- Off-line scheme
  -The offline model is a fully offline and portable system.

- User is fully anonymous unless double spend
  - The user is as anonymous as the online system if and only if they did not double spend.

- Bank can detect double spender
  - The ID of the double spender would be revealed, this is an advantage towards the bank as it might worries about double spending problem.

- Banks don't need to synchronize database in each transaction.
  - The frequency of the synchronization between the bank servers is kept to a minimum as these are always done via batch updates.

- Coins could be reusable
  - Depending on the implementation, coins in the system could be reusable which further reduces the overhead and the size of the coin in the database.

### Cons

- Might not prevent double spending immediately
  - As the user could in theory still double spend by risking the chance of being caught. (The chance is really high indeed!)

- More expensive to implement
  - The extra security hardware needed in the system requires an additional cost.

## Blind Signatures

The idea of blind signatures is to make someone e.g. the bank, without them know the content of what they are signing. The use of this would allow the anonymity property required by digital cash systems. This idea was invented and patented by David Chaum [1]; you could argue that David Chaum was the farther of blind signature. David Chaum also invented the protocol that uses it; (presented later) has been used as a base of further improvements by many researchers, the improvements are normally ‘add-ons’ to the original proposal made by David Chaum.

So, how do blind signatures work? First let’s see what the problem is, for example:

1. **You use a RSA system to hash a message *m* and sent to the bank: $H(m)$**

2. **Using its secret key *d* and *n*, the bank signs the message: $H(m)^d \bmod n = r$**

3. **Now the customer *c* can spend this money *r* and the merchant *s* will verify that this is valid by asking the bank to decrypt it, but what if the bank kept a record of this and to whom it was given. The bank would now know *r* was given to this customer *c* and spent at merchant *s*, thus were you spent your money.**

To allow the bank to sign the message without them know what it is, uses an additional element called a ‘blinding factor’ *b*:

1. **You would now send $r = H(m)b^e \bmod n$**
   **(where *b* is a random number ($1 \leq b \leq n$) know to the customer but not the bank, and *e* is the banks public key)**

2. **The bank would again sign this: $r^d = (H(m)b^e)^d \bmod n$**

3. **The bank could again keep a record of this, however you would prevent is by removing the binding factor**

4. $$\begin{aligned} r^d &= (H(m)b^e)^d \bmod n \\ &= (H(m)^d b^{\cancel{ed}}) \bmod n \\ &= (H(m)^d b) \bmod n \end{aligned}$$

5. **Now, remove the blinding factor by $b^{-1}$ → $H(m)^d \bmod n$, this is now the same as the money generated without using blinding however the bank does not have a record of this.**

## Untraceable digital cash

You may be wondering that the bank has just signed something that without knowing what it was; this is where the protocol comes in (DigiCash, founded by David Chaum, uses this as part of its implementation). This protocol preserves the anonymity by using blind signatures and a cut-and-choose method.

The protocol goes:

1. **The customer would create *k* units of money *m*. The money would contain some header information, the denomination and a different serial number in each. The serial number is randomly generated and would be long enough so that collision does not take place (e.g. 64-bit serial number has a probability of collision of $1/2^{64}$). So the money would have the format:**
   **$m_1$ = (header info, denomination, serial number), …, $m_k$ = (header info, denomination, serial number).**

2. **The customer would then blind each of them with a different binding factors *b*, using the banks public key *e*: $m_1b_1^e, \ldots, m_kb_k^e$, and sent to the bank for signing.**

3. **The bank randomly chooses *k*-1 of them to check, and leaves one unit *i***

4. **The bank cannot check the contents of them because of the blinding factor, The customer gives the bank all the blinding factor except the one for unit *i***

5. **The bank can now check the content to make sure the customer has not tried to cheat (e.g. by putting £10 instead of the agreed £5). There is still a chance that the bank would not check the unit that is fraudulent but the probability of this happening deceases as you increase the size of *k***

6. **If all checks out the bank would sign the remaining unit with its private key d and send it back to the customer: $(m_ib_i^e)^d = m_i^db_i$**

7. **The customer would un-blind it by using the inverse $b_i^{-1}$ to leave $m_i^d$**

## Secret Splitting

Secret splitting is a method used to split a message into n parts. Each part on its own is useless, but when all parts are combined the original message will be revealed. A one-time pad is used to implement this. A one-time pad generates random strings of numbers that are used as a key. This key is then XOR with the message to produce the different parts. For example, if the message is 2510, and the key generated is 1500, the message can be split in the following way: **2510 XOR 1500 = 3090**

The two parts are now 1500 and 3090. They are useless on their own but when they are XOR together, i.e. **1500 XOR 3090 = 2510 – the original message is produced**

## How is this used within the protocol?

A coin will contain the following:

- Serial number – a unique number that identifies the coin
- Denomination – the actual value of the coin
- Validity Period
- Transaction list – has an arbitrary number of transaction items.

A transaction item is created when the coin is transferred between the customer and the merchant. Each transaction item consists of n identity strings. The identity refers to the identity of the owner of the coin.

Each identity string consists of two parts, P1 and P2. P1 and P2 are the results of secret splitting. From the example above, P1=1500 and P2=3090. A different value for K is used for each string. For example, the transaction item for user with id 2510 may have the following:

| **P1** | | **P2** |
|---|---|---|
| 1500 | | 3090 |
| 4545 | | 6159 |
| 5878 | | 7992 |
| | ..… | |
| | ….. | |
| 4791 | | 7033 |

If P1 and P2 are XOR the original id of the user will be revealed,
e.g. **4545 XOR 6159 = 2510**

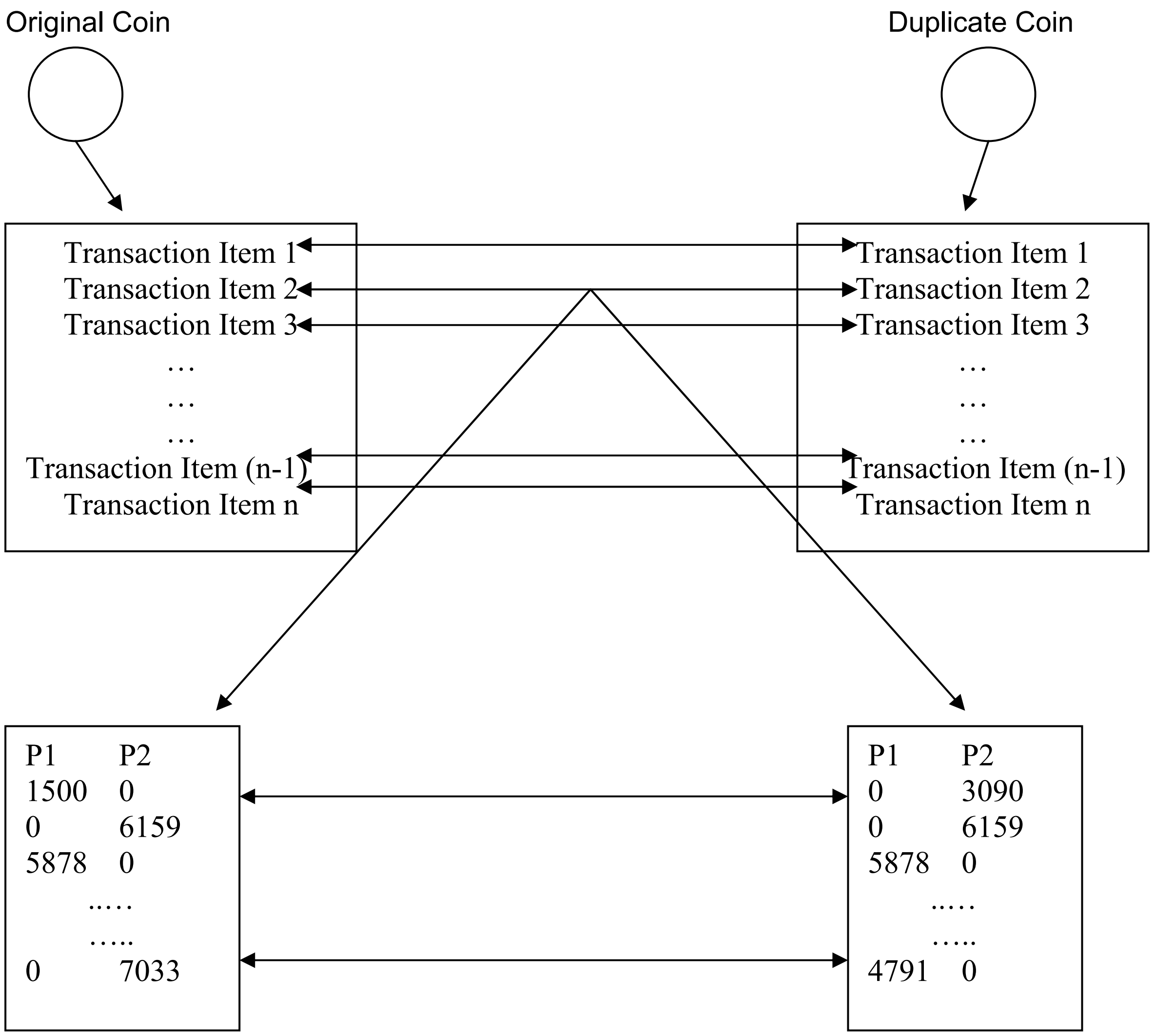
When a user spends their money, the protocol will randomly blank some of P1 and some of the P2, ensuring there is no pair of P1 and P2 remaining and therefore the owner of the coin cannot be identified, i.e.:

| **P1** | | **P2** |
|---|---|---|
| 1500 | | 0 |
| 0 | | 6159 |
| 5878 | | 0 |
| | ..… | |
| | ….. | |
| 0 | | 7033 |

The protocol will then add a new transaction item with the new owner of the coin's id encoded on it. It will leave all the pairs visible to show who the owner of the coin is.

**<u>How does this detect double spending?</u>**

If a user makes a copy of a coin before they spend it, they have the possibility to spend that coin again. However, when the coin is finally returned to the issuer, it will be possible to discover the culprit. This is achieved by combining a particular part of the identity from the original coin with its corresponding part from the copied coin. Note that the corresponding part will have been blanked out in the original coin. For example, let's assume user with id 2510 makes a copy of a coin and spends it twice. The diagram below shows exactly how double spending is detected:



| P1 | P2 |
|---|---|
| 1500 | 0 |
| 0 | 6159 |
| 5878 | 0 |
| ..… | |
| ….. | |
| 0 | 7033 |

| P1 | P2 |
|---|---|
| 0 | 3090 |
| 0 | 6159 |
| 5878 | 0 |
| ..… | |
| ….. | |
| 4791 | 0 |

At **transaction 2** the user made a copy of the coin and spent it elsewhere. Once the coin finally reached the issuer, they can match up pair of corresponding P1 and P2 to reveal the identity of the user who has spent the coin twice.

**1500 XOR 3090 = 2510 or 7033 XOR 4791 = <u>2510</u>**
(Notice that <u>2510</u> was the id of the user)

## The probability of catching a user

The probability of catching a user depends on the number of identity pairs used in the transaction. The more pairs used, the greater the chance of catching the culprit. The probability of catching the culprit is:

$$1-\tfrac{1}{2}^{n}$$

Where n is the number of pairs used.

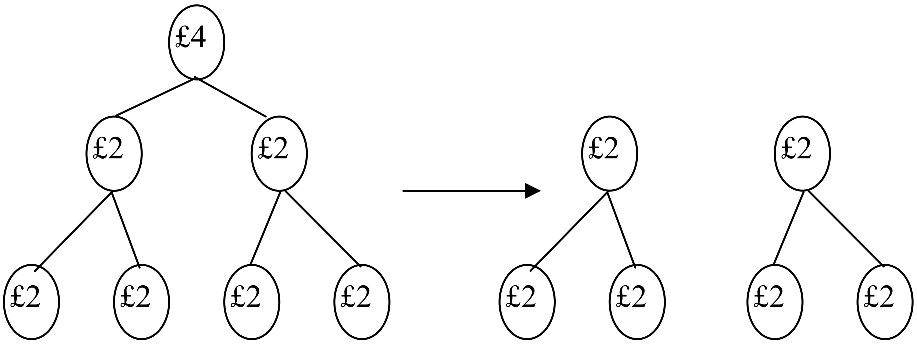
Example, if n=5 then the chance of catching a user is 0.97.

## Memory requirements

By allowing more than one person to use the same coin, there will be extra data appended to the coin 'file'. As you may have guessed, the size of this file will be ever growing. A possible solution to this is to have a maximum number of transactions. This would limit the number of ID's added to the file. No more transactions can take place once the maximum has been reached, and the coin must be banked.
Also to prevent the banks database of serial numbers there maybe a validity period (or expiration date) associated with the coin, and then the coin will no longer be able to be banked. This would allow the bank to 'clean-up' its database of invalid serial numbers.

### Other proposals

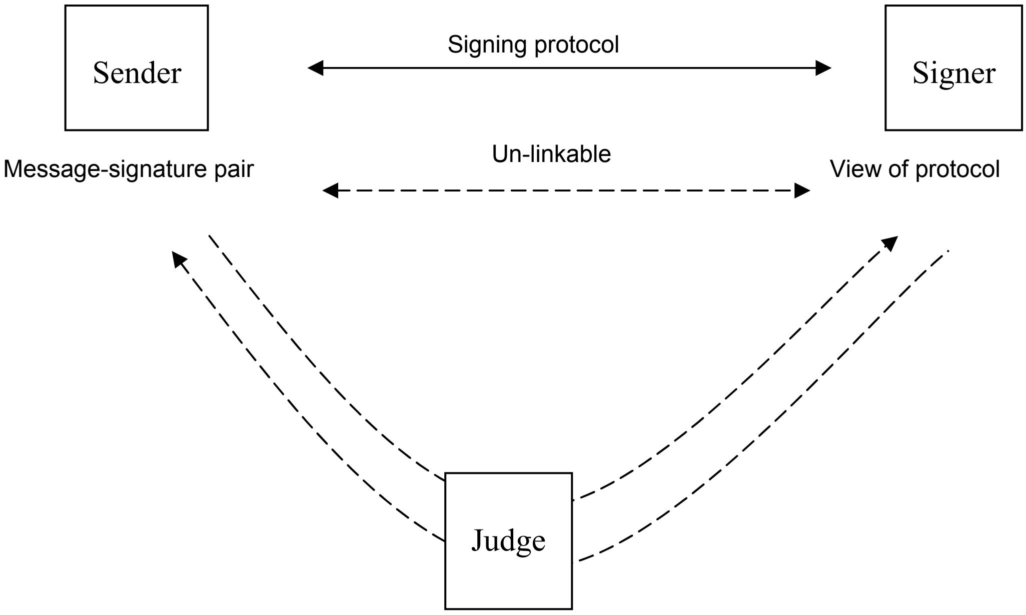
There are also other problems involving memory, for example each coin would need a file, and if you carry a lot of change there would many files and so, it would take up more memory.
There have been other proposal that use different protocols; a possible solution to the problem above is to use a tree structure to represent the amount of money. The user would then be able to spend a 'branch' from the file, as the diagram below shows:



## Fair blind signatures

There is a lot of concern regarding the anonymity of digital cash with respects to illegal activities. For example it can be used for money laundering and ransom demands without being able to trace the culprit. Fair blind signatures are a group of proposals/solutions that overcome this intractability.

One of these solutions is to have a trusted third party in the transaction on money. In the below diagram it is called a judge. The judge would have access to either the massage-signature pair or the signer's view of his protocol. With this information and the information from either the sender or signer the culprit can be traced.



## Conclusion

The elimination of physical cash from our economy is already feasible from a purely technological perspective. The economic barriers are also disappearing, though a substantial additional investment in equipment and cards would be needed to permit even purchases such soft drinks to be made.

But transactional privacy will be at the heart of the government's attack on digital cash. Because it’s untraceable, the government concerns about money laundering, offshore banking and tax havens, and has been closely monitoring developments of digital cash. The government would probably only license the company’s patents in a way that preserved the ability to trace for law enforcement purposes. Without the government support, the investors don’t have confident in the development of digital cash. DigiCash, a pioneering firm in the area, attracted only $160k US dollar in two years, declared bankruptcy in 1998 and bought by eCash Technologies. Now eCash is having its own troubles and bought by another company call InfoSpace.

## Overall advantages of digital cash

E-cash is basically software; it can be programmed to do things that paper money could never do. This ability opens up a whole range of exciting functionality that money may offer. Besides this, there are many other advantages on offer.

### 1. For the Users:

**1.1 Convenience.** One of the most apparent benefits of digital cash is convenience. Users may access funds, pay for items or be paid from the comfort of their home. With smart card implementation, users will also be able to initiate financial transactions wherever they may be. Cell phones are being developed to process electronic cash transactions; this will ensure convenience reaches unimaginable heights. Not only is such ease of use desirable, but it saves time and effort and inevitably money. Such capability will also empower the disabled, making them more competitive in the financial world.

**1.2 Security.** 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. Another important benefit for the user is improved security. Passwords for 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 include biometric information of the user. Current security standards are already competitive, it is claimed that consumers are 11 times more likely to have their credit card number stolen by a waiter than they are from an unsecured internet transaction.

**1.3 Intractability.** The primary advantage digital cash promises over other electronic payments are anonymity. True anonymous digital cash would also provide unconditional intractability. 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.

## 2. For the Bank:

**2.1 Less Processing.** Single transactions need not be authorized on line, debited from the customer's account or printed for the customer. This greatly reduces processing effort, meaning time is saved and less staff is required

**2.2 Security.** With the security measures built into the electronic wallet, fraud costs and costs for clarifying disputed transactions could be reduced. Nowadays, card fraud is a very important problem. The same applies to card counterfeiting and forged bank notes.

**2.3 Handling.** Handling costs for paper cash are exorbitant. This includes guarding, transporting, counting, storing and the like. With weightless cash bereft of any volume, these massive savings will be made.

## 3. For the Retailer:

**3.1 Time saving.** The instantaneous quality of electronic transactions, means retailers accounts will be credited for immediate use if necessary.

**3.2 Transaction Costs.** 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. Costs for counting, storing and transporting cash would also decrease.

## Global Disadvantages:

**1. Safety.** The safety of any system is only as strong as its weakest link. German national television recently showed how a hacker could create a Web page, with an embedded ActiveX control, that is able to snatch money from one bank account and deposit it into another, bypassing the customary personal identification number that is meant to protect theft.

**2. Algorithm.** Most algorithms used in these monetary systems have been around for many years already. Numerous cryptology experts have attempted breaking them without success. However, one can never rule out the possibility of a security break in the future.

**3. Physical Securities.** Another weak spot is the user’s personal hardware (e.g. the smart card) and his copy of the software. Only complete physical security can guarantee the safety of the stored money. There are some skeptical of the physical safety of the smart card chips.

**4. Economic Disruption.** 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 system. Economists also predict that speed and ease of e-cash will increase monetary velocity which in turn will cause unnecessary inflation.

**5. Users.** 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. This is an often underestimated topic as user confidence is the key to the success of digital cash. 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.

**6. Legal problems.** Digital cash's untraceable nature will loosen government's control over financial information. Money laundering and tax evasion could proliferate in stateless e-money systems. A major fear is that criminals will take advantage of such systems to aid illegal activities.

Conversely, an effort to regulate e-cash by removing anonymity will infringe on the financial privacy of users. Electronic systems offer promising automatic auditing ability to governmental institutions. Critics, therefore expect resistance from government in establishing financial confidentiality. The U.S. government has already unsuccessfully attempted to force a privacy-intruding "Clipper chip" onto the industry. In France cryptography is completely forbidden by the law. Obviously this is currently an area of heated debate.

## References

1. David Chaum Amos Fiat and Moni Naor, "Untraceable Electronic Cash", in Advances in Cryptology - CRYPTO '88 Proceedings

2. David Chaum, “Blind Signature System” US Patent #4759063

3. Pater Wayner, "Digital Cash Commerce on the Net", Academic Press Inc 1996

4. Hitesh Tewari, Donal O'mahony & Michael Peirce (1998). “Reusable Off-Line Electronic Cash Using Secret Splitting”, Technical Report TCD-CS-1998-27, Trinity College Dublin Computer Science Department, Dublin.

5. Paul Sprague, “Blind Signatures and Fair Blind Signatures”
http://www.csh.rit.edu/~spraguep/crypto/

6. Digital Cash Mini-FAQ
http://ntrg.cs.tcd.ie/mepeirce/Project/Mlists/minifaq.html

7. Cashless Society or Digital Cash?
http://www.sfasu.edu/finance/FINCASH.HTM

8. Digital Cash and Net Commerce
http://www2.pro-ns.net/~crypto/toc12.html

9. Digital Cash
http://www.simovits.com/archive/dcash.pdf

10. Anonymity & Privacy: The InternetCash TM Example by Yiannis Tsiounis, Ph.D.
http://www.internetcash.com/fgo/0,1383,white02,00.html

11. Digital Cash and Blind Signatures by Zhihao Chen

12. ELECTRONIC MONEY & DIGITAL CASH by Michele Pelossi
http://vrm.vrway.com/issue13/ELECTRONIC_MONEY_DIGITAL_CASH.html

13. InfoSpace
http://www.infospace.com