DIGITAL CASH

Presented by:

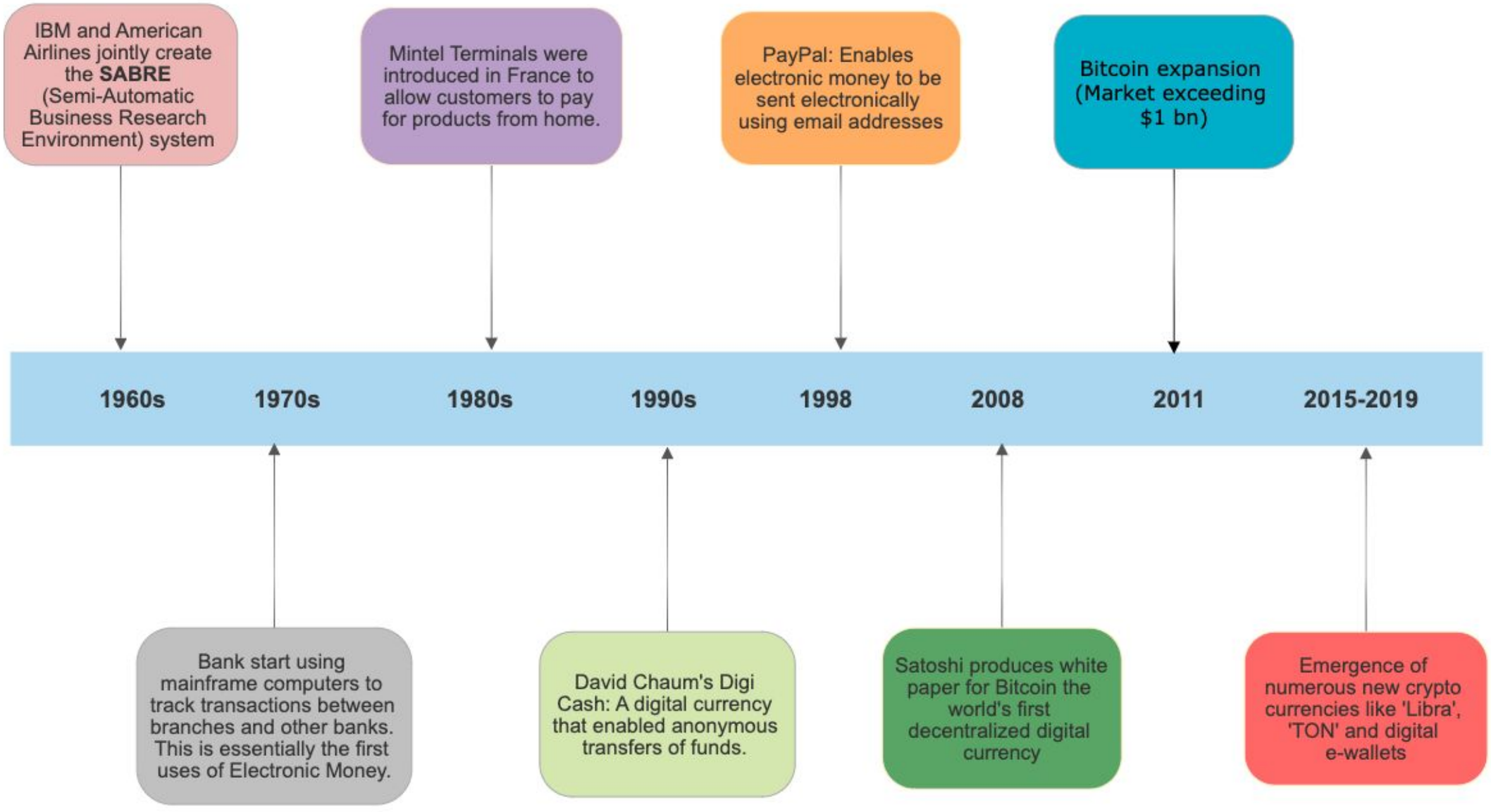
1. **Neha Suresh Kamthe**
2. **Pragati Sharma**
3. **Aysha Siddhikha Husaini Basha**
4. **Koushik Kumar Kamala**

Under the guidance of : Prof. Gokay Saldamli

WHAT IS DIGITAL CASH?

- Digital cash is a system of purchasing cash credits in relatively small amounts.
- A payment message bearing a digital signature which functions as a medium of exchange or store of value.
- Need to be backed by a trusted third party, usually the government and the banking industry.
- Digitally Signed payment message.
- Storing that credits in the personal computer and then spending them while making electronic purchases over the internet.
- CIA triad

Timeline of Digital Cash

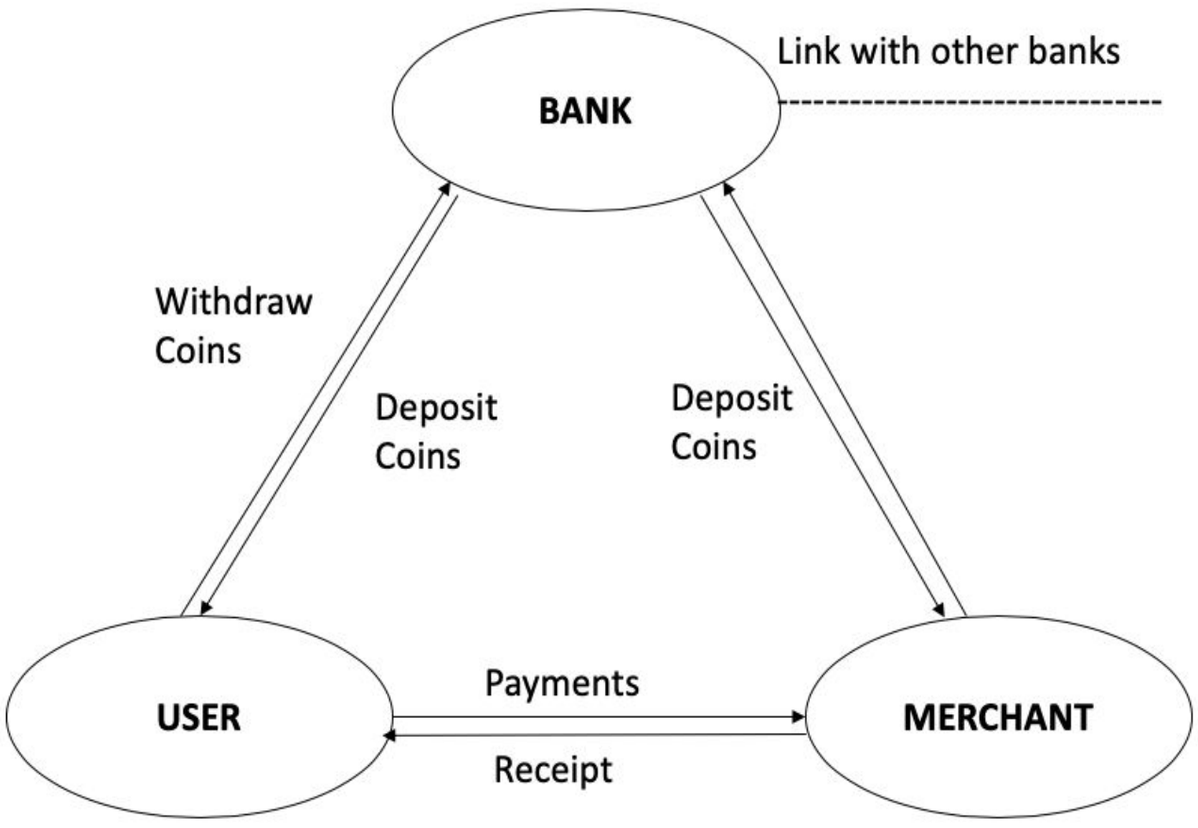


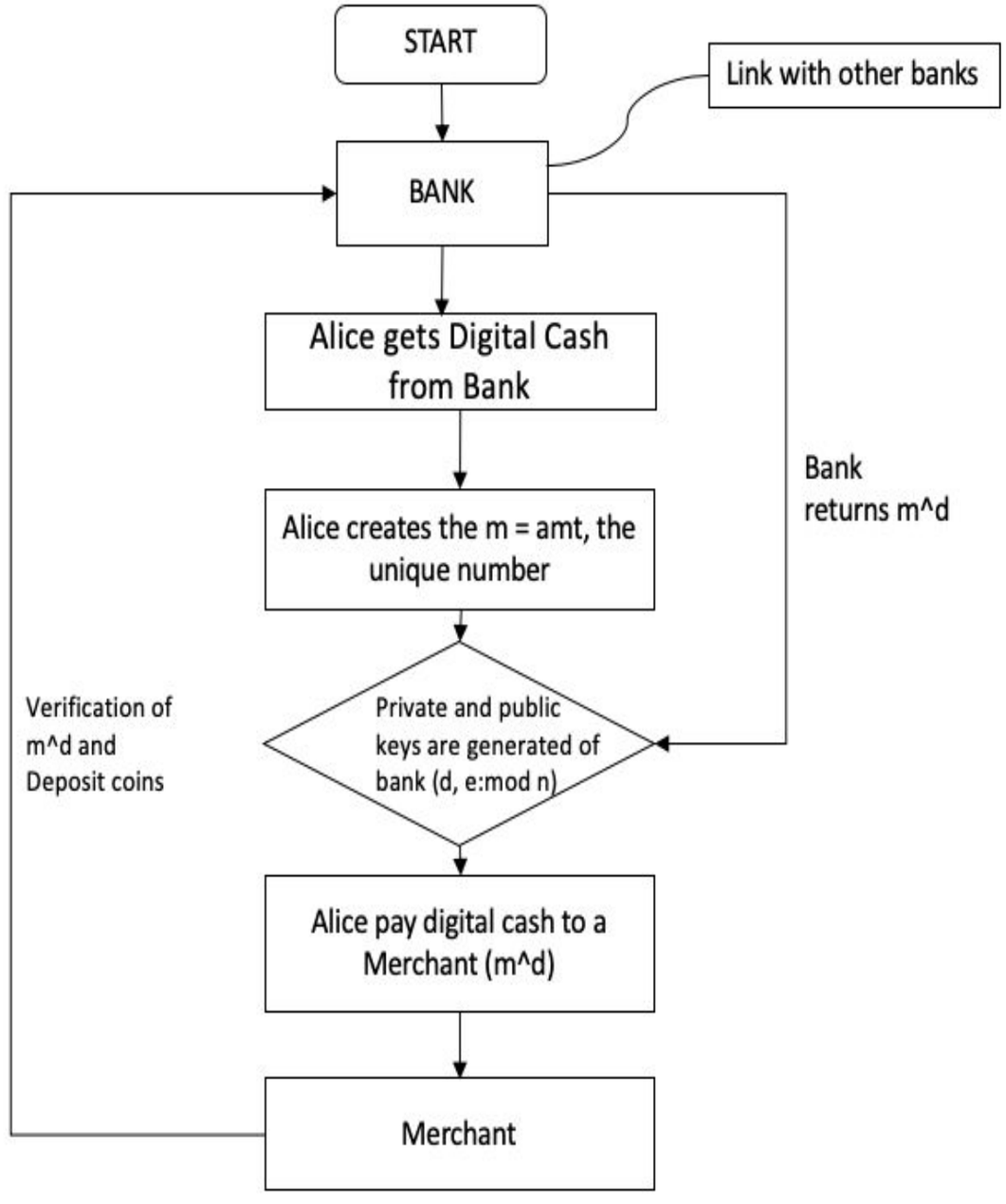
Salient Features of digital cash

Types of digital cash

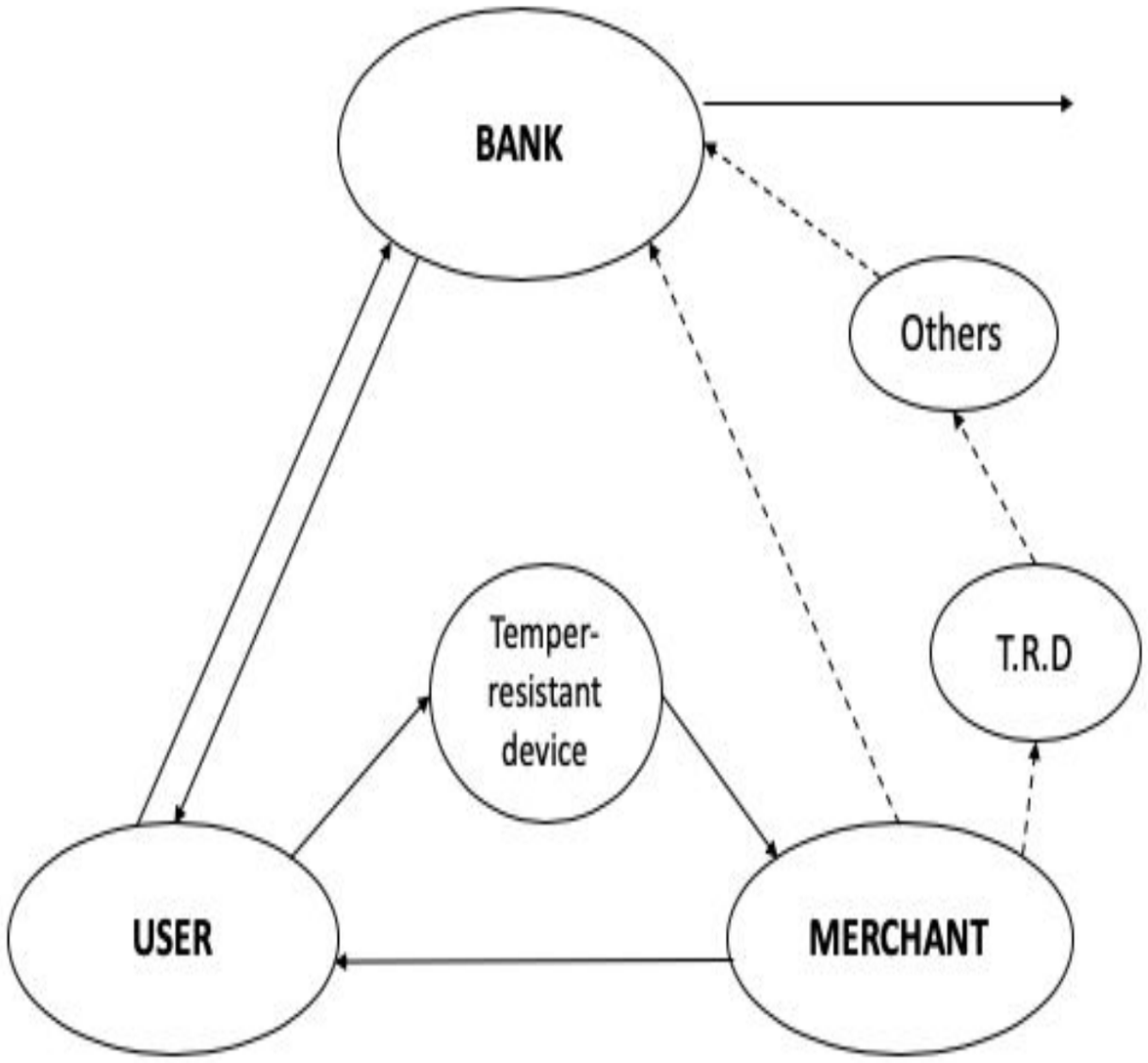
1. Traceable Online Digital Cash.
2. Untraceable Online Digital Cash.
3. Traceable Offline Digital Cash.
4. Untraceable Offline Digital Cash.

Traceable Online Digital Cash





Traceable Offline Digital Cash



- Blind signatures are used when a user wants the individual to sign something without knowing what they are going to sign.
- This procedure is carried out using multiplying the message by a unique number or secret number called as binding.
- The individual signs the blinded message.

PROTOCOLS IMPLEMENTED

1. Blind Signature

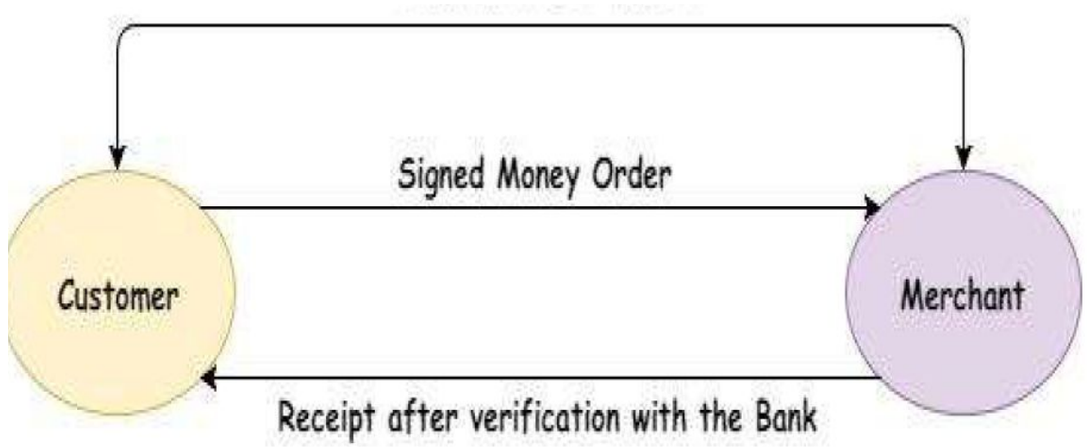
- Customer wants to have Bank sign in message M.
- Bank's public key is (e, n). Bank's private key is d.
- Customer picks a blinding factor b between 1 and n.
- Customer blinds the message M by computing
  $M' = M\ b^e \pmod n$ sends M' to Bank.
- Bank signs M' by computing
  $S' = (M\ b^e)^d \pmod n = M^d\ b \pmod n$
- Customer unblinds this by dividing out the blinding factor:
  $S = S' / b = M^d\ b \pmod n / b = M^d \pmod n$
- But this is the same as if Bank had just signed M, except Bank was unable to read M'

2. Secret Splitting

- A method that splits the MO's into n parts.
- Each part on its own is useless but when combined will reveal the MO.
- Each MO is XOR with a one time Pad, R

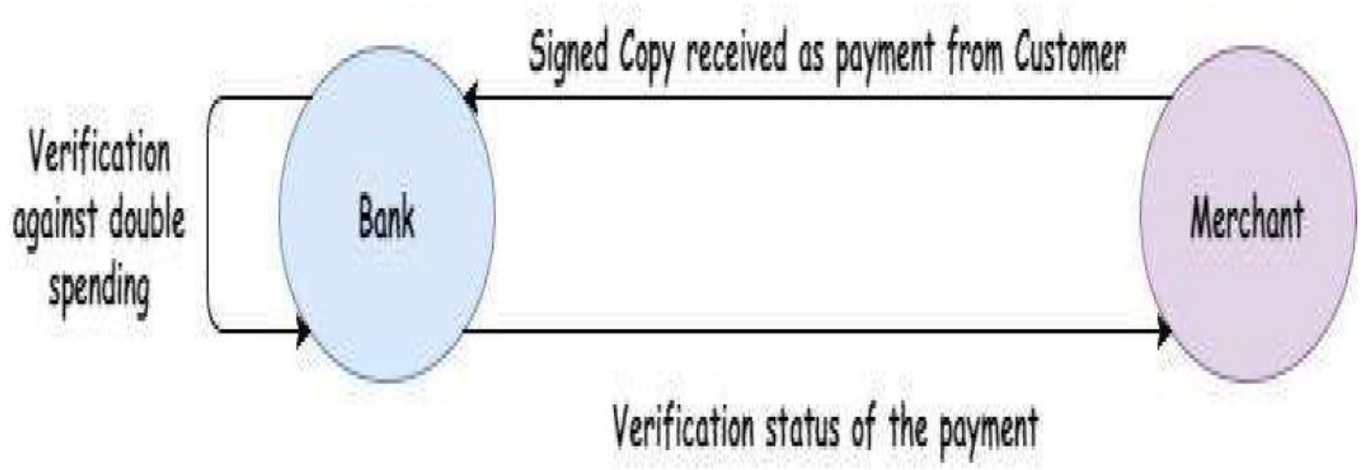
3. Bit-Commitment Protocol

- Customer wants to “commit” number M to Merchant.
- Customer picks a random nonce r (to prevent replay attack) sends Merchant y = H(r || M) (H is a one-way hash) and now customer cannot change it.
- When Merchant wants to know M, Customer sends M and r.
- Merchant H(r || M) and sees if it equals to y. If so, M was in the commitment y originally



Double Spending as a problem

- Customer stays anonymous.
- If Customer spends a coin twice, then will be identified.
- If Merchant deposits twice, then caught but Customer remains anonymous.
- Must be secure against Customer and Merchant cheating the bank together.
- Must be secure Customer or Merchant making it look like the other is cheating.



Advantages

- It provides fully anonymous and untraceable digital cash. The spent cash is not associated with any particular user.
- The transaction is totally in real-time so coins are verified, thus, no problem of double-spending takes place.
- The hardware requirements for the additional feature is not much.
- Long-distance transaction is simpler. The cost to send money internationally (worldwide) and to persons on the side (in the neighborhood) is the same in digital cash.

Disadvantages

Double spending was one of the biggest problems. However, this was solved using different electronic tokens.

- The transaction taken place are not traceable as digital cash uses the internet as a platform for communication.
- Forgery can also take place using hacking. Hackers may break the system as the cash is in digital form.
- The communication between bank and merchant should be verified properly so that there is no double money spent.
- Every time it is necessary to generate new strings for every transaction. This makes usage of resources a lot and allocation is very high.
- Synchronization is important thus merchants and banks have to be updated with special software. This problem is related to scalability.
- The huge database is required to store strings, which makes the rate of data transmission slow.

References

1. http://users.telenet.be/d.rijmenants/en/secretsplitting.htm
2. https://mrajacse.files.wordpress.com/2012/01/applied-cryptography-2nd-ed-b-schneier.pdf
3. http://www.dmi.unipg.it/~bista/didattica/sicurezza-pg/sistemi-pagamento/e-cash-payment.v1.10.20.pdf
4. http://faculty.bus.olemiss.edu/breithel/b620s02/riley/Digital%20Cash-Web%20Page.htm
5. https://www.w3.org/Conferences/WWW4/Papers/228/
6. https://medium.com/@FidelityDigitalAssets/the-evolution-of-digital-cash-da19b06aa58e
7. https://journal.binus.ac.id/index.php/comtech/article/view/2399/1825
8. https://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS4/DigitalCash.html

Thank You