Digital Cash

Neha Suresh Kamthe
Electrical Engineering
San Jose State University
nehasuresh.kamthe@sjsu.edu

Aysha Siddhikha Husaini Basha
Electrical Engineering
San Jose State University
ayshasiddhikha.husainibasha@sjsu.edu

Koushik Kumar Kamala
Computer Engineering
San Jose State University
koushikkumar.kamala@sjsu.edu

Pragati Sharma
Computer Engineering
San Jose State University
pragati.sharma@sjsu.edu

***Abstract*—With the swift development of the computer and network and information technology, transaction-based digital cash has replaced the traditional check transaction. In recent years, the main concern is the operational efficiency and safety aspect of the digital cash system. The digital cash is intangible. The paper proposes an understanding of protocol such as blind signature, secret splitting for digital cash. The digital cash is a collaboration of traditional cash and traditional cash in today's world. This system does not provide any trace of the transaction between the sender and receiver of money which is the drawback of digital cash. This is called as double-spending. Thus, digital cash is ease related to e-cash and cryptocurrency.**

***Index Terms*—Digital cash, Blind signature, Secret Splitting, Double spending**

I. Introduction

"David Lee Chaum (born 1955) is the inventor of many cryptography protocols, as well as E-cash and DigiCash. His 1981 paper, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", laid the groundwork for the field of anonymous communications research. The first electronic payment was sent in 1994". Digital cash transactions have become commonplace by the year 2000. The major difference came in digital cash when Satoshi Nakamoto wrote a paper about Bitcoin in 2008 where Peer to Peer Electronic Cash system was introduced. However, there a number of protocols used which are the blind signature, secret splitting, commitment and it is unclear which ones are dominant. There is still a problem with double-spending in digital cash. Each digital exchange begins with a taking a bank that issues money numbers or other unique novel identifiers that convey a given worth, for example, ten dollars. To get such an authentication, you should have a record at the bank; once you purchase digital cash certificates, the money is pulled back from your account. You give your unique code to the vendor to pay for a product or service, and the vendor deposits the unique code number or the identification code in any participating bank or re-transmits it to another vendor. For huge purchases, the merchant can check the validity of a unique code by contacting the issuing bank.

The paper consists of three main parts: Bank, Merchant, and Customer. The digital cash has online and offline modes that are associated with all three parts. Types of digital cash are :

- Traceable Online Digital Cash.
- Untraceable Online Digital Cash.
- Traceable Offline Digital Cash.
- Untraceable Offline Digital Cash.

II. Traceable Online Digital Cash

Following shows the online traceable structure of digital cash transfer.

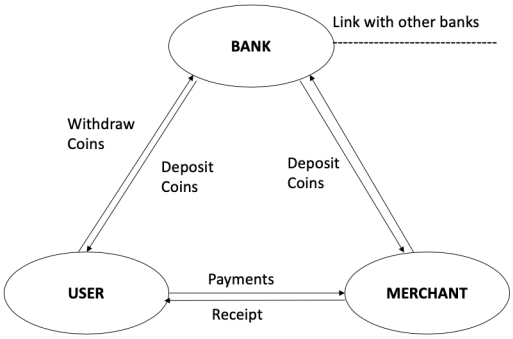

Fig. 1. Cash Flow in Digital Cash in Online mode.

A. Spending and depositing coins

"These methods are straight forward. To spend the coins, simply offer them to the vendor. To reclaim them, simply offer them to the bank. The bank will check its legitimacy and credit your record. To tackle the double-spending problem, the trader needs to confirm the coin with the bank at the purpose of offer in every one of the exchanges. This check of the authenticity of the coin requires additional transmission capacity and is a potential bottleneck of the framework particularly when the traffic is high. The real-time verification also means there is a need for the synchronization between bank servers".

III. Untraceable Online 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

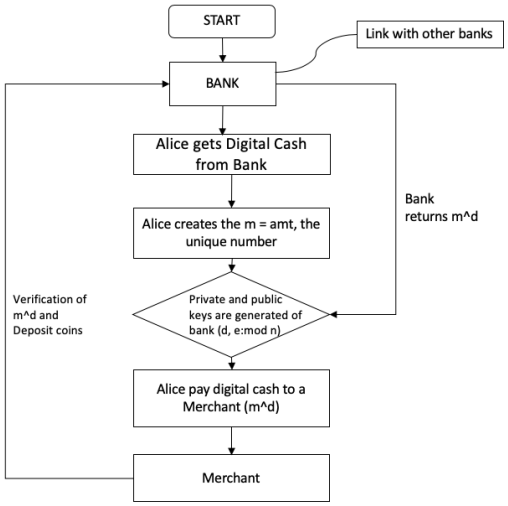

Fig. 2. Flowchart for Digital cash online.

message by a unique number or secret number called as binding. The individual signs the blinded message.

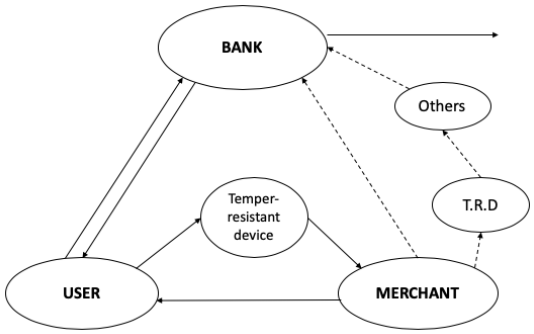

Fig. 3. Cash Flow in Digital Cash in Offline mode (Untraceable).

A. Blind Signature

A bank can create digital keys (public and private) by signing a message which specifies the number and value of the note. Bank sends signed MO to the customer and the customer sends MO to the merchant. Thus, merchant deposits in the bank and get verification and status of the payment. Blind signature and secret splitting are together implemented to achieve anonymity and integrity. The Customer can send M message in n secret pairs. The bank signs one money order randomly from n pairs and asks the customer for their remaining corresponding blinding factors to verify.

- The customer wants to have the Bank sign in the message M.
- Bank's public key is (e, n). Bank's private key is d.
- The customer picks a blinding factor b between 1 and n.
- Customer blinds the message M by computing

$$M' = M.be(modn) \tag{1}$$

sends M' to Bank.

- Bank signs M' by computing

$$S' = (M.be)d(modn) = Mdb(modn) \tag{2}$$

- Customer unblinds this by dividing out the blinding factor:

$$S = S'/b = Mdb(modn)/b = Md(modn) \tag{3}$$

- But this is the same as if Bank had just signed M, except Bank was unable to read M'

B. Secret splitting

Secret Splitting enables to leave password or code in the custody of multiple persons without disclosing the secret. In Secret Splitting, * Secret information is split into several parts. Both shares are required to obtain the initial information that was used for division into left and right strings, and if one of the shares is not valid, it is mathematically impossible to acquire the original information. The data obtained from multiple shares does not help in uncovering any information or partial information about the entity nor does it help to recover the entity information in any way. We can not simply cut the secret information into two, of course, as this would expose at least half of our original information and ultimately can lead to total transparency of the original information.

- Let the secret key be a number R (randomly generated)
- The message is XORed with the R
- The Money order is split into R and the result
- The message is obtained when the key (R) and the result are XORed together

Ultimately, there's another very important property in Secret Splitting. Since the system is unbreakable, the loss of one portion will always lead to the substantial loss of the secret information, if not the owner still has a copy of the original.There is no way back if a share is lost or destroyed by accident! Therefore, it might be useful for the owner to have an extra copy of the original information, or for the share-owners to have a copy of their share, somewhere in another secure location. And, of course, if you break secret information into shares and plan to dispose the original data, be sure to double-check the shares as we stand a chance of no way to get back the original message.

C. Bit-commitment protocol

The customer has a signed money order from the bank and reveals to the merchant using HMAC. The merchant has to confirm that the customer is transferring the money order as promised earlier. The implementation uses a one-way and collision-free hash function.

- The customer wants to "commit" number M to Merchant
- Customer picks a random nonce r (to prevent replay attack)
- The customer sends Merchant

$$y = H(r||M) \tag{4}$$

HMAC is a one-way hash using SHA256 and now a merchant cannot change it.

- When Merchant wants to know M, the Customer sends M and r.
- Merchant H(r —— M) and sees if it equals to y. If so, M is in the commitment y originally

IV. Double Spending

- Customer stays anonymous.
- If the Customer spends a coin twice, then it 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.

V. 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.

VI. 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.

VII. Results

Results for digital cash program using python 3.7. with Mac OS terminal as environment are as follows:

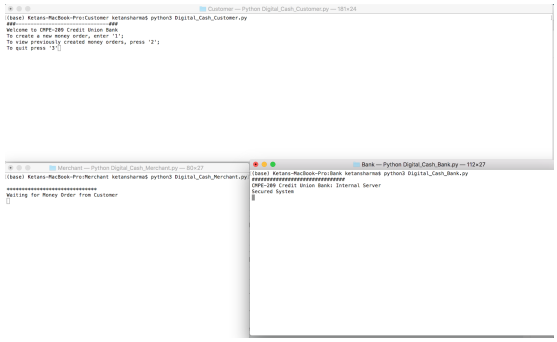

Fig. 4.

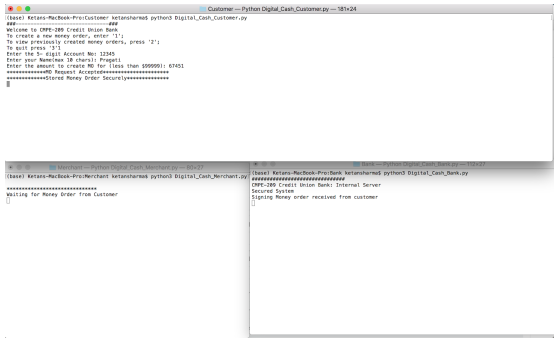

Fig. 5. Customer creates ‘m’ number of MO.

A. Initial/default state of each functions (see Fig. 4)

B. Successful money order creation by Customer(see Fig. 5)

C. Successful payment debited by merchant from bank(see Fig. 6)

D. Error Scenario: Customer copied the MO and used twice(see Fig. 7)

VIII. Conclusion

Successfully implemented offline digital cash system . Using blind signature and secret splitting, the anonymity of the customer is ensured. The security of the system is implemented using RSA 2048 encryption. We understood the features such as prevention of double spending, and identification of fraud or hacker detection. In conclusion digital cash is cryptocurrencies in the form of stablecoins. These can be backed by fiat currencies issued by governments on a 1 to 1 ratio thus imitating our own traditional currencies. It allows for fast transactions, low fees, and even more security, transparency and convenience.

IX. Future scope

- The digital cash can be secured from DDos attacking.
- Two-step verification for double spending.
- Providing common synchronization tool for all entities.

References

[1] https://en.wikipedia.org/wiki/Blind_signature

[2] http://users.telenet.be/d.rijmenants/en/secretsplitting.htm

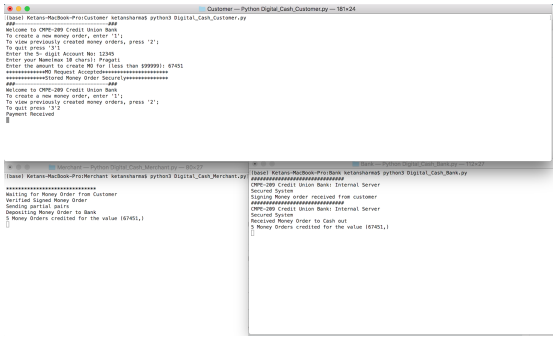

Fig. 6. Initiation for the money order is started by customer and cash out is initiated by bank.

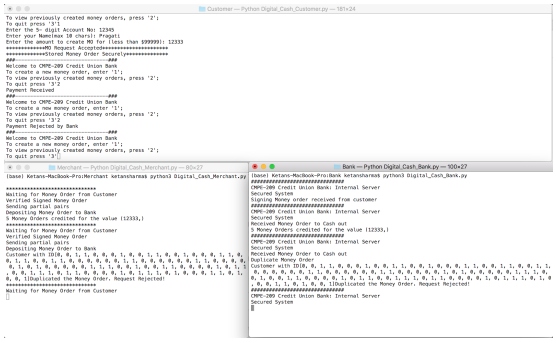

Fig. 7. Payment received by merchant, still it tries to double spend it thus, bank gives the error and duplicate message is displayed.

[3] https://mrajacse.files.wordpress.com/2012/01/applied-cryptography-2nd-ed-b-schneier.pdf
[4] http://www.dmi.unipg.it/bista/didattica/sicurezza-pg/sistemi-pagamento/e-cash-payment.v1.10.20.pdf
[5] http://faculty.bus.olemiss.edu/breithel/b620s02/riley/Digital
[6] https://www.w3.org/Conferences/WWW4/Papers/228/
[7] https://medium.com/@FidelityDigitalAssets/the-evolution-of-digital-cash-da19b06aa58e
[8] https://journal.binus.ac.id/index.php/comtech/article/view/2399/1825
[9] David Chaum - Wikipedia. https://en.wikipedia.org/wiki/David_Chaum
[10] https://www.webopedia.com/TERM/D/digital_cash.html
[11] http://www.cs.bham.ac.uk/ mdr/teaching/modules06/netsec/lectures/DigitalCash.html
[12] http://rageuniversity.com/PRISONESCAPE/COMMUNICATION%20CODES%20AND%20INKS/secret_splitting.pdf