



ISSN: 2319-5967

ISO 9001:2008 Certified

International Journal of Engineering Science and Innovative Technology (IJESIT)

Volume 4, Issue 2, March 2015

Electronic money- A way of convenience for making transaction over internet

Yash chugh

Abstract- Now days, making transaction in mainly done over internet which provide users with the convenience ease to use and other benefits. Making payments over internet is possible with the use of electronic money system which makes customer to make payments for different goods by sending files from one computer to another. These files are money in form of computer files. In 1990, David Chaum founded DigiCash, an electronic cash company. The first electronic payment was made in 1994.

Index Terms - e-money, blinded factor, transaction, digicash.

I. INTRODUCTION

Electronic money is mainly that can have many different meaning but in principal with the use of involvement of computer networks, its digital values and digital systems to store and making payments over internet[1]. Electronic money can be or theoretical, historical or current. Electronic money is mainly digital cash stored in form of computer files and retrieved for any payment over internet.

Simply electronic money is mainly making the transaction of money with digital system on the computer networks as on internet. Electronic money can include making transaction, fund transfer, billing system over internet, digital currencies, fund deposit etc. An electronic transaction is any kind of non-cash payment that does not engage the paper check. Electronic money is supposed as a way of storing and transmitting money through digital systems or as electronic cash which is makeable as a currency [2] in its own right.

Electronic money is a system that allows a person to pay for goods or services by sending a number from one computer to another computer. Like the serial numbers on real dollar bills [3], the digital cash numbers are unique and different for each. Each one is issued by a bank and represents a particular sum of real money. Electronic money is nothing but money which is in form of computer files as physical form of cash is replaced with binary form of computer data.

II. PROPERTIES OF SUPREME ELECTRONIC CASH SYSTEM

- A. Independence-** electronic cash is not dependent on any physical location. The cash can be set through computer networks over internet from one computer to another.
- B. Security-** The digital cash can't be copied and reused when once it is spent over.
- C. Untraceability -** The confidentiality of the user is protected as no one can trace the relationship between the user and his purchases for anything.
- D. Transferability-** The electronic cash can be transferred to other users over internet.
- E. Divisibility-** A quantity of electronic money in a particular amount can be subdivided into smaller parts of money in smaller amounts.

To obtain the electronic money one must have his account in the bank. Most of electronic money system starts with the bank that issues the cash number or any other unique recognition that carries a specified value, such as ten dollars.

III. KINDS OF ELECTRONIC MONEY

Electronic money is mainly classified in two parts as follows-

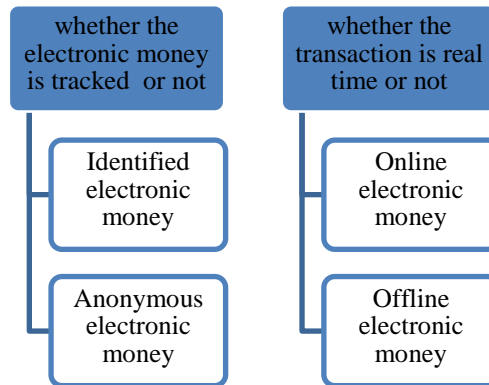


Fig. 1. Classification of electronic money

First classification is according to whether the electronic money is tracked or not-

A. Identified electronic money

Identified [4] electronic money mainly contains information enlightening the person who originally withdrew the money from the bank. In identified e-money, the money issued by the bank to any customer and final return of that money to bank is fully traced by the bank itself. Bank pays tracking element for the money as bank knows that who is the original customer who requested for money and where and how he spent that money. For making the electronic money identifiable it contains a unique serial number [5] which is generated by the bank itself. Thus the bank has the list of different serial numbers for the electronic money which is requested by different customer. For example, credit card transaction is also a type of online e-money.

Steps involved in identified electronic money-

1. Suppose the consumer requested the e-money to bank worth \$500 then bank will give the e-money to consumer worth \$500 with serial number which is generated by the bank itself say SN500.
2. Consumer sends this electronic money to the merchant along with the serial number.
3. The merchant would go back to the bank for redeem the money and to get the real money instead.
4. The bank will have the same electronic money with serial number as SN500

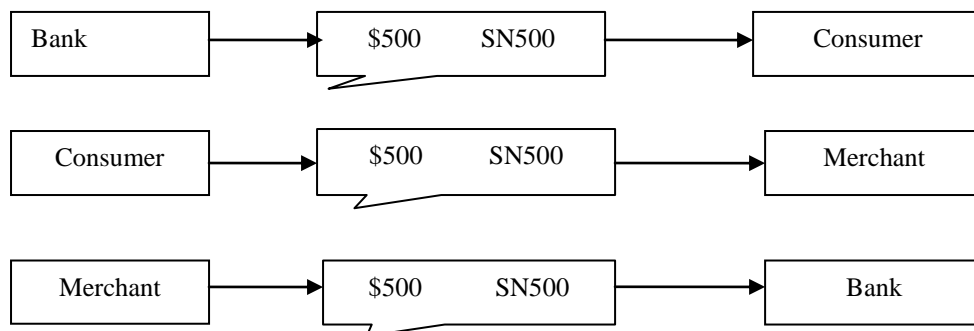


Fig. 2. Fig: steps involved in identified e-money

B. Anonymous electronic money

The anonymous electronic money [6] mainly works like real hard money. There is no trace of the money which was spent and also there is no trail of the transaction which is involved in anonymous e-money. The key difference between anonymous and identified e-money is, where in identified e-money, serial number is created by the bank but in case of anonymous electronic money, and serial number is generated by the customer itself. Process for use of anonymous e-money involves the use of blinding factor. Money fraud can easily be trace in

case of anonymous e-money as the bank can maintain the list of the issued and spent different serial numbers Example for the anonymous e-money is Digi-cash [7].

Steps which are followed in anonymous e-money are:-

1. Consumer generates the random number by using some mathematical operation and which is multiplied by some huge number which is known as blinding factor.
2. The consumer sends the blinding number to the bank
3. The bank does not have knowledge about the original number as it consider the blinding number as original number
4. Bank authenticate the number and send it back to the consumer
5. The consumer than replaces it's blinded number with the original number using some algorithm and sends the original number to the merchant.
6. The merchant encashment to bank with the original number which is given by consumer to merchant as in step 5
7. The bank cant trace the e-money as they does not know about the relation between the original number and the blinded numb

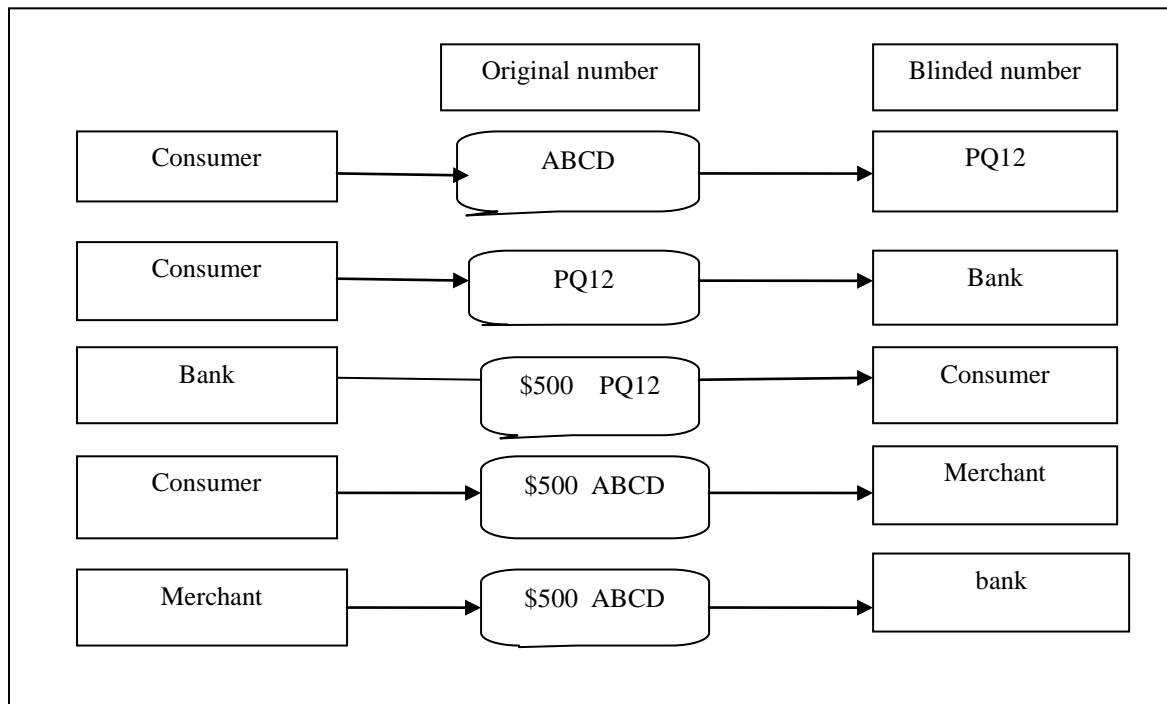


Fig.3. steps involved in anonymous e-money

Classification based on the involvement of bank in transaction

A. Online electronic money

In online e-money, the bank pays the role of participant in transaction between the customer and merchant. Thus before the completion of the transaction, the merchant would confirm to bank as the money sent by the customer is acceptable or not.

B. Offline electronic money

In offline e-money [8], the bank does not actively participate in the transaction between the customer and merchant. The customer sends the e-money to merchant and merchant accept that money without verifying money at that time. The merchant might collect a group of e-money and process that together at a fixed time each day.

IV. SECURITY MECHANISM IN ELECTRONIC MONEY

The process of consumer obtaining the money in the form of files from the bank. A consumer buying anything from merchant and then sending these files to him in replacement of real hard money.

- Suppose that customer requested the e-money for \$500 from bank and bank giving the same as with encryption of original method with its own private key.
- Bank then encrypt the encrypted[9] message with consumer public key and send to consumer

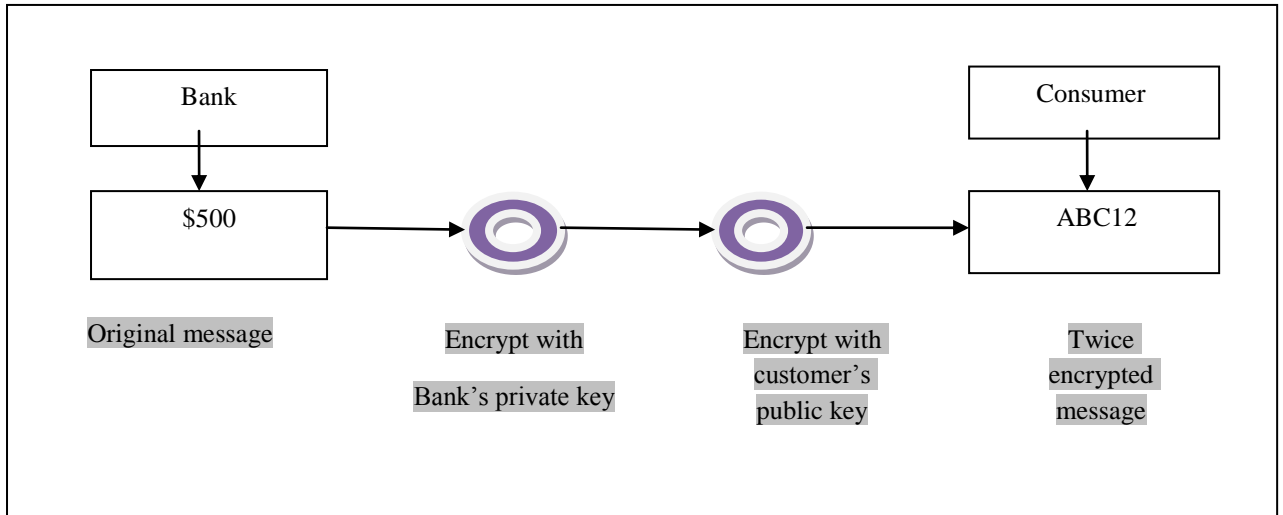


Fig.4. bank sends the e-money to consumer after encryption it twice

- Consumer receives the encrypted money and decrypts the message with its own private key.
- Consumer again decrypts the message with bank's public key. Thus the consumer gets the original message of \$500 after decryption.

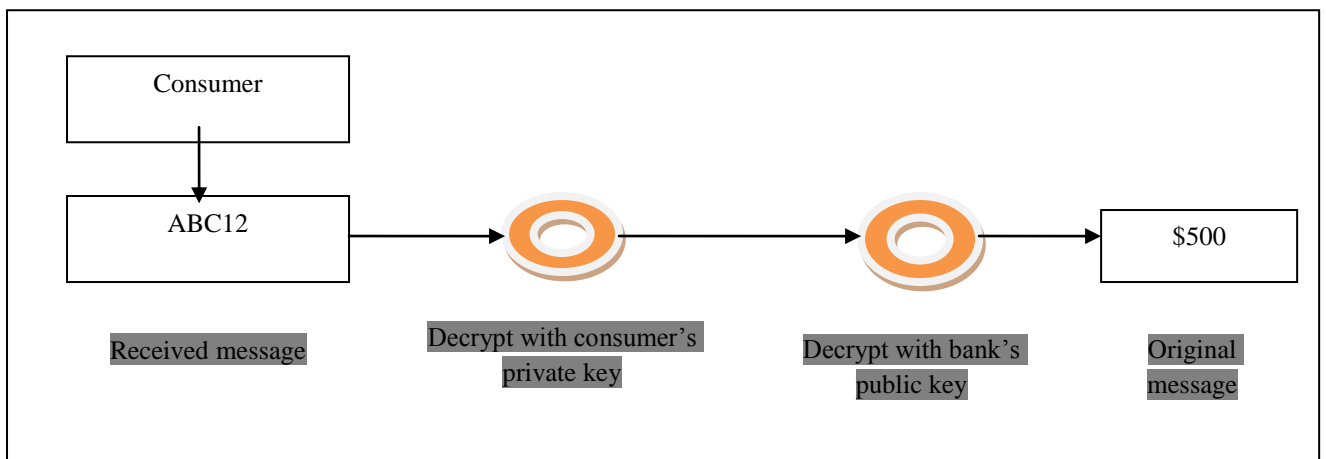


Fig.5. consumer decrypts the bank's message twice to get e-money

V. ISSUES NEED TO BE UNDERTAKEN

- Consumer Related Issues
 1. Net needs to safeguard their privacy and transactions.
 2. Security: Acknowledgement assures the customer that their transaction was not diverted or otherwise misplaced.



ISSN: 2319-5967

ISO 9001:2008 Certified

International Journal of Engineering Science and Innovative Technology (IJESIT)

Volume 4, Issue 2, March 2015

3. Any system of electronic money will also need to instill complete confidence of transaction protection and currency soundness.
 4. Regulation: standardize digital money.
- Business Related Issues: availability of internet, make the business the possibility of global reach. The considering facts for business are:
 1. Availability of anonymity to the customers or business who purchase through digital money.
 2. Cost and ease of gaining
 3. Cost of ease of online/offline verification
 4. Availability
 5. Risk of fraud (double spending, stolen money, fraudulence)
 6. Liability for fraud

VI. CONCLUSION

This paper concludes the importance of electronic money. Identified and anonymous electronic money that provides secure transmission of money over internet with and without involvement of bank from consumer to merchant for the payments of goods. This paper presented a classification of different type of properties of using electronic money transaction. Proposing electronic money system security is always a challenge.

REFERENCES

- [1] "Applied Cryptography" – "6.4 Digital Cash" by Bruce Schneier.
- [2] <http://www.sims.berkeley.edu:8000/courses/is204/f97/GroupE/>.
- [3] <http://www.ex.ac.uk/~RDavies/arian/innovation.html>.
- [4] <http://www.ftc.gov/bcp/conline/pubs/online/payments.pdf>.
- [5] <http://www.res.org.uk/society/mediabriefings/pdfs/2003/april03/markose.asp>.
- [6] <http://www.transaction.net/press/tomorrow.html>.
- [7] <http://www.chyp.com/digmon/default.asp>.
- [8] "How DigiCash Blew everything" <http://www.jya.com/digicrash.htm>.
- [9] <http://www.ex.ac.uk/~RDavies/arian/emoney.html>.

AUTHOR BIOGRAPHY



Yash chugh received the B.tech degree (with first class honors) in information technology in 2013 from N.C institute of engineering and technology affiliated from Kurukshetra University. And presently pursuing M.tech in computer science from N.C institute of engineering and technology. Her interest area is network security and image processing. Currently she is working on study of ad-hoc network. She has published two technical papers in national and international conferences and one technical paper in international journal.