REVIEW OF RESEARCH
ISSN: 2249-894X
IMPACT FACTOR : 5.2331(UIF)
VOLUME - 7 | ISSUE - 6 | MARCH - 2018

CASHLESS SYSTEM IN MODERN BUSINESS-EVOLUTION OF ELECTRONIC TRANSACTIONS

S. Nandhinipriya
Student, Department of Business Administration,
Theivanai ammal college for women, Villupuram.

ABSTRACT

India is trying to leapfrog into digital, it has a long way to go. Sweden, South Korea, Denmark, Canada have high percentage of cashless transactions—as high as 75-85%. Norway has stopped cheques. Of course, these countries are either smaller, or have a more educated population, higher penetration of organised retail and higher awareness about digital than India. India continues to be driven by the use of cash; less than 5% of all payments happen electronically however the finance minister, in 2016 budget speech, talked about the idea of making India a cashless society, with the aim of curbing the flow of black money. This paper focused on the importance and problems of cashless economy and electronic transaction. It is observed that India has almost half-a-dozen methods for cashless payments. And yet users can't leave home without cash. Demonetisation accelerated a shift to digital payments, but will take lot more time to become the prime payment option.

KEY WORDS: *Cash less economy, Digital Cash, Electronic transactions* **.**

INTRODUCTION

The present day payments fall into two large categories: accounts-based system and token -based system. Token-based system such as paper cash, pre-paid phone cards or mail stamps, do not identify its user. A pre-paid phone card, for example, does not distinguish one caller from the other. Account-based system such as check, credit card or bank accounts need, by design , to identify the system users and their transactions. People like to use paper cash because it is easy to carry around, they can make a payment with the received cash and they don't need to ask a third party like a bank to perform their payment. Paper cash can, however, be stolen or lost and no one compensates for the lost or stolen money. Credit card reduces risk of lost cash for people, but by using electronic money people are in the risk are losing their privacy. Annually, credit card companies and banks lose large sums of money since they are required to compensate for lost card and the costs associated with fraud and human error.

In light of the explosive increase of electronic services such as internet, the need for more efficient electronic payment has become an essential fact. Since anonymity of payments is usually associated with anonymity of paper cash, anonymous token-based electronic payment system is referred to as digital cash (also known as electronic cash, E-cash, D-cash). Digital cash offers a solution to the problem of paper cash and today's credit card , it is secured and protect people's privacy. The customer can use digital cash to pay over the internet without the involvement of a bank during their payment. The goal of this report is to present a few of the present day digital cash systems, discuss their properties, provide a comparison and determine

them together to see which one of them fulfills the properties for digital cash and the required security level. This report also presents and understanding of the method that the chosen system can be applied in practices. In addition this report tries to be a bridge by building a bridge between the gap of research and real-life application. This paper focused the problem and prospectors on online electronic payment system.

GENERAL STRUCTURE OF DIGITAL CASH TRANSACTION

There are three different types of transaction during a digital cash procedure:

a) Withdrawal, in which Alice transfers some of her money from her bank account to her wallet(Could be a smart card or a personal computer).
b) Payment, in which Alice transfers money from her wallet to BOB's.
c) Deposit, in which bob transfers the money he has received to his bank account.

In a digital cash system we have three kinds of actors:

- A financial network
- A payer or consumer
- A payee or a shop

IMPORTANT PROPERTIES OF DIGITAL CASH

Digital cash is designed to construct an electronic payment system modeled after our paper cash system. Therefore digital should have same features as paper cash like: recognizable hence readily acceptable, transferable, untraceable, anonymous, and portable and has the ability to make "change" (some people like okamato believe that even the paper cash is undividable. Here we present in detail some necessary properties of digital cash.

- **Security** With security we mean that digital cash cannot be copied and reused. Then we have to minimize the risks for forgery and established a good authenticity system.
- **Forgery the** most obvious risk with any payment system is forgery or counterfeiting. As with paper cash we two kinds forgery in a digital cash system.
- **Token forgery** to create a valid-looking coin without making a corresponding bank withdrawal.
- **Multiple spending** using the same token over again. Multiple spending is also commonly called re-spending, double-spending, and repeat-spending.

To protect against token forgery, one release on the usual authenticity functions of user identification and message integrity. To protect against multiple spending, the bank maintains a data base of spend electronic coins. coins already in the data bash are to be rejected for deposit. If the payments are on-line, this will prevent multiple spending. if off-line, the best one can do is to detect when multiple spending as occurred. To protect the payee, it is then necessary to identify the payer. Thus it is necessary disable the anonymity mechanism in the case of multiple spending.

Authenticity:

As a consequence of the problems of forgery, it becomes necessary to establish various levels of authenticity measures.

- User identification: user must know with whom he is dealing with.Message integrity: to be sure that the copy of the message is that as same as it was in the beginning.
- Non repudiation: to protect against later denial of a transaction.The authenticity future are attained via key management. Key management is carried out using a certification authority (CA) a trusted against who is responsible for conforming a user's identity. Without a trust CA and a secure infrastructure, the security features of digital cash will be practically impossible over an entrusted transmission medium like internet.

Privacy:

The definition of privacy is not really clear. For some people privacy means protection against eavesdropping but for others like David chum policy means anonymity for the prayer payment and

untraceability of the payment just that the bank cannot tell whose money was used in a particular payment. Just as cash is anonymous ,digital cash anonymous in that it cannot be traced back to a particular individual, it is considered to be "unconditionally untraceable". However, the service provider is assured of it's authenticity , all that is missing is the ability to link the transaction with a particular person. if a user's coin linkable, we can identify the user by finding a single payment in which the user as identified himself. Then a digital cash system will protect user's privacy if it is both unlikable and untraceable. Digital cash systems that don't pay attention to privacy or "privacy-invading systems" virtually all commercial systems currently being proposed are privacy-invading. They emphasize the bank's security, but pay little attention to the security of the customer (in terms of protection from financial surveillance). Anonymity increase the danger with money laundering, illegal purchasing, blackmailing and counterfeiting that are far more serious than with paper cash. Anonymity would increase the danger of these problem. More anonymity means less security and vice versa.

Portability:

The security and use of digital cash is not dependent on any physical location. The cash can be transferred through computer network into storage devices and vice versa.

Transferability:

Transferability allows a user to spend a coin that he has received in a payment without having to contact the bank. A payment is transfer if the payee can use the received coin in a payment. A payment system is transferable if it allow at least one transfer per coin. We have to notice that the ability to transfer paper cash is very important in our daily life.

The Problem Which Appear With Transferable System Are:

- Any transferable electronic cash system has the property that the coin must grow in size each time it is spent because of the information it has to contain. This information is about every person who has spent the coin for the bank to maintain its ability to catch multiple spenders. This limits the maximum number of transfers allowed in the system by the allowable size of the coin.
- Money laundering and tax evasion are hard to detect since no records of the transaction are available.
- Each transfer delays detection of multiple spending or forged coins. Multiple spending will not be noticed until two copies of the same coin are deposited and it may be too late by then.
- Users can recognize their coin if they sees it later in another payment.

Divisibility:

With divisibility we mean the ability to make change. So digital cash will come in cent or smaller denominations that can make high-volume, small-value transaction on the internet practical. A solution for divisible coins is using coins that can be divided to coins whose total value is equal to the value of the original coin. This allows off-line payments to be made without the need to store a supply of coins of different denominations.(observe that okamoto believes that even normal paper cash can't satisfy this characteristic by being divisible).

Off-line payment:

Off-line line payments means that bob submits Alice's electronic coin for verification and deposit some time after the payment transaction is completed. It means that with an offline system Alices can freely pass value to bob at any time of the day without involving any third party like a bank. Although off-line systems or preferable from a practical view point, they are however susceptible to the multi-spending problem and their fore suitable for value transactions low. Over the past years, some off-line cash systems have been designed that can not only guarantee security for the bank and shops, but also privacy for the users.

On-line:

On-line payments means that bob calls the bank and verifies the validity of Alice's token by a simple question like "have you already seen this coin" before accepting her payment and delivering his merchandise. On-line payment remains necessary for transaction that needs a high value of security. With an on-line

system, the payment and deposit are not separate steps. On-line systems require communication with the bank during each payment, which costs more money and time (communication cost, database-maintenance costs and turn-around time);however the protocols are just simplification of off-line protocols. Since on-line system have to be able to check the credibility of prayers for shops, it is almost impossible to protect the anonymity of its users, besides as on-line system require communication with a third party during the payment transaction, then we can not have transferable coin if the system is an on-line one.

Digital signature:

Digital signatures were first proposed in 1976 by Whitfield Diffie. A digital signature is the electronic equivalent of a hand-written signature. The key aspects of both types of signature are that only one person or service-provider is capable of producing the signature and all others are capable of verifying it. A digital signature guarantee that anyone reading a digitally signed message can be certain of who sent it. Digital signature employ a pair of keys,a private key, used to sign message and a public key, used to decode them. Only a message signed by the private key can be used, decoded and verified using the public key. In this way one can create a digital signature, equivalent to a hand-written signature on a document. Since a digital signature is not physically connected to the signed data or the originator, it depends on this data and on the secret key of the originators. Several signature schemes have been proposed. The RSA public-key crypto system can be used for both enciphering and digital signature. Schemes which can only be used for digital signature purposes are the DSA and the fiat-shamir scheme.

Digi-cash:

Digi-Cash was founded and created by David Chanum in 1990 and is located in Amsterdam. It develops and license payment technology products. One of the company's products is ecash, a prototype for digital cash which has been in progress since 1995. This system is designed for secure payments from any personal computer to any other work stations, over mail or internet. Ecash is implemented almost around chum's digital cash system, however the main difference is that e-cash is an on-line system.

How e-cash works inside?

Each person using e-cash has an account at a digital bank on the internet, for example EU bank in Finland. Using that account people can withdraw and deposit e-cash. E-cash is a coin based system, which means that digital money is implemented by digital signatures representing a certain fixed amount of money. E-cash security is based on the RSA encryption keys. Every person or entry using e-cash has a unique pair of keys. One key is kept secret (the secret key) and the other key made public (the public key). Alice who wants to authenticate a message encrypts it with her own secret key, everyone can verify that Alice signed this message by decoding it with the Alice's public key. If Alice wants to send a confidential message, encrypts the message with the public key of the receiver is the only one who will able to decode the message. When an e-cash withdrawal is made, the PC of the user calculates how many digital coins and of what denominations are needed to withdraw the requested amount. The PC generates random serial numbers for those coins, which will act as the coin's serial number and a blinding factor is included. The blinding factor is required so the bank is not required to maintain a list of the coin's serial number and discover where the money is spent. The result of these calculations will be sent to the digital bank.

The bank will first verify the message and then encode the blinded numbers with its secret key (digital signature), at the same time debiting the account of the client for the same amount. The authenticated coins are sent back to the user and finally the user will take out the blinding factor that he introduced earlier. The serial numbers plus their signatures are now digital coins their value is guaranteed by the bank. The coins can be stored locally on the PC of the user. As soon as he wants to make a payment, his PC collects the coins needed to reach the requested total value. These coin are sent to the receiver, then the receiver sends them directly to the digital bank before he accepts your payments. The bank verifies the validity of these coins and they have not been spent before. The account of the receiver is credited. Every coin is used only once. Another withdrawal is needed if the receiver wishes to have new coins to spend.

E-cash works like travel checks if you lose it, you have to report this to your bank and supply them with the serial number of the lost coins, then the bank can check if the coin are really lost and refund them. A user

can cancel a payment if she is not satisfied with her shopping by revealing the coins serial number to the bank and asking them for payment cancellation. The system advantages are privacy for prayer, low transaction cost and the ability of person to person payments. This system provides anonymity for prayer since the coins are created with blind signatures on the withdrawal protocol. (however if users use their own serves for the payment protocol, then the payment is not completely anonymous for them since the payee will have knowledge of their internet address. The payers can keep their anonymity by using a forwarding agent.) The payment is not private for payees, he must turn the coins immediately to the bank to determine if the coins are valid, before delivering the sold item to payer. Digicash argues that this form of payment protocol minimizes the ricks of double spending.

Administration Problems

Administration problems are that kind of problems which must be solved before a digital cash product could take off. Today exist some of these problems by some of digicash actors. The most important one of these problems is to keeping an on-line service. We remember that one of major advantages with digital cash is that people can pay their payment fast and effective this problem appears when some of the actors like the EUnet of finland can not have an on-line service for the customers. The customers should wait approximately a week in some cases even longer to get their accounts open or get answer for an usual question like how they could open an account. Sometimes it create marketing problems in the segmentation of services providers (vetrivel, 2017)

CONCLUSION

This system offers the possibility to generate different denominations and currency, hence, the system offers two different ways to denote the coin value. The coins generated by this system are secure and provides their user's anonymity. Band presents the alternatives of his system to generate portable coins the only drawback of brands system is the high communication, which can however be lowered by asking the user to withdraw several coins at the same time. However, even brands cash system is neither divisible nor transferable (notice: he offers an alternatives to creating a divisible system on the cost of anonymity and implementation of this system cause some problems which are not easy to solve. So even this system does not fulfill all the requirements of an ideal digital cash system. Different companies like digicash are known to have tried for generating a digital cash system but none of them have been successful because of security problems implementation problems and administration problems, "if a coin is lost who suffers the loss?" must be solved before digital cash could be as common as paper cash is today.

REFERENCES:

- ✓ "The history of Money" Jack Weatherford. Crown publishers, inc. New York 1997
- ✓ "The Story of Money" Norman Angell. Frederick A. Stock Company, New York 1929
- ✓ http:// www.webopedia.com/TERM/D/ digital_cash.html
- ✓ http:// moneycentral.msn.com/content/banking/creditcardsmarts/P74808.asp
- ✓ http:// en.wikipedia.org/wiki/octopuscard
- ✓ Playing with plastics David Evans and Richard Schmalensee. MIT press, Cambridge Massachusetts 2005.
- ✓ Vetrivel .V(2017). A Study on Marketing Problems of unorganised retail shoppers", International journal of multidisciplinary research review, volume 1, issue 31,1-5, Sep 2017.

S. Nandhinipriya
Student, Department of Business Administration , Theivanai ammal college for women, Villupuram.