Research Paper

Volume : 2 | Issue : 10 | October 2013 • ISSN No 2277 - 8179

e-Cash- Electronic Cash Payment: a System without Use of Paper or Coins

Computer Science

KEYWORDS : Internet, Information & Communication Technology(ICT), Electronic Cash (e-Cash)

Dr. Sudhakar D. Bhoite Asso.Professor, Dept. Of Computer Studies, SIBER, Kolhapur, MS, India.

ABSTRACT

In this 21st century the Internet has made revolutionary impact on all aspects of human life. Out of all, banking operations have greater impact of ICT on its day-today happenings. An e-cash payment system is one of the evidence of impact of internet and information Communication technology jargons. In this process a consumer/client opens an account with the banking organization or other which could give and receive money in the digital coins form. In the case client's account is deposited in the form of real money, as it is attached to the client's checking account in reality.

Introduction

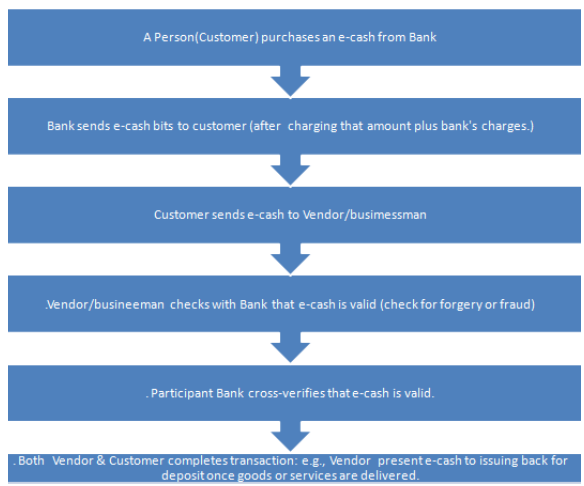
An E-cash or Electronic cash is a kind of system which permits a consumer(person) to make payment for objects/goods or services by a way of transmitting a number from one computer(PC) to another(PC).as in similar the serial numbers on real currency notes, these digital cash numbers are unique one. Each number is issued by a bank and represents a specific amount (sum) of money. Un-like the real cash it is anonymous and reusable ie when digital cash is sent from a consumer to a seller, there is no way to get information about the buyer. This way of payment ie. Digital cash transactions have now become more common. In to-days scenario most of digital cash systems start there functioning with a involving bank, which issues cash numbers or other unique identifiers which carries a specified value, for eg. €5 Thus to get such a certificate ,the person must have an account in the stated bank; when the person purchase digital cash certificates the money is withdrawn from persons' account. Thus an E-cash or electronic cash is digital money that is used for online purchasing. To perform e-cash transactions, users need specific software on his/her PC to enable him/her to download money from their bank account into their cash wallet on their PC. In the process of buying, customers perform an exchange with the downloaded money with the vendor for the product they make a purchase. The vendor afterwards redeems the sought money in a bank which accepts e-cash deposits ref:. www.webopedia.com

An E-Cash is a term that indicates a kind of a storage of a value and exchange concept used and created by a person which don't make use paper documents or coins for buying services. This type of system may work as an alternative means for government-issued physical currency notes and coins.

Process Of E-Cash

In an e-cash transaction the consumer is required to download and install a software called electronic wallet on his/her computer(PC). So, as to get DigiCash, an electronic wallet is used by consumer to create digital coins, and thus, these created coins are sent to the bank to get signed. And after the coins are signed, the equivalent amount of money is withdrawn from the person's (customer's) account of concerned bank. In case of when the person interested in making a purchase, he/she suppose to send signed digital coins to the Vendor. On the contrary the a vendor cross-verifies the bank's signature and performs the deposit of the coins into the bank, where they are credited to the vendor's account in the respective bank.

Phases In An E-cash Transaction:



Risks Involved In E-Payment Transactions:

A vendor is likely to misuse information provided by customer for making transactions, or even he/she could malfunction with consumer's site, steal information related to consumer, and misuse by the way of e.g.,Vendor may quote higher prices on the bases of past behavior of consumer. From consumer's point of view following risks are involved:

- If consumer is a competitor then attempts to learn prices or strategies.
- May be a could an imposter, and will not make bill payment.
- Sometimes a consumer seems to be a hacker then can: make changes what is get ordered by bona fide customers; changes what prices are charged; make changes what is available; steals customer contact information and likewise.

Features Of e-Cash Concept:

- E-cash means substituting cash as the principal, payment medium in customer-oriented electronic payments system.
- Even though 'cash' is still the most prevalent customer payment instrument even an evolutionary developments in electronic payment modes.
- 'Cash' factor remains the dominant form of payment for three reasons:
- lack of trust in the banking system; inefficient clearing and settlement of non-cash transactions; negative real interest rates paid on bank deposits.
- The predominance of cash indicates an opportunity for innovative business practice that revamps the purchasing process where consumers are heavy users of cash.
- To really displace cash, the electronic payment systems need to have some qualities of cash that current credit and debit cards lack.
- Cash is legal tender, meaning the payee is obligated to take it.
- Also, cash can be held and used by anyone even those who don't have a bank account, and cash places no risk on the

part of the acceptor that the medium of exchange may not be good. If you compare cash to credit and debit cards.
- First, they can't be given away because, technically, they are identification cards owned by the issuer and restricted to one user.
- Credit and debit cards are not legal tender, given that merchants have the right to refuse to accept them.
- Nor are credit and debit cards bearer instruments; their usage requires an account relationship and authorization system.
- Similarly, checks require either personal knowledge of the payer or a check guarantee system. Hence, to really create a novel electronic payment method, we need to do more than recreate the convenience that is offered by credit and
- debit cards.
- We need to develop e-cash that has some of the properties of cash.

Properties of e-Cash
- Specifically, e-cash must have the following four properties: monetary value,
- interoperability, irretrievability, and security.
- E-cash must have a monetary value; bank authorized credit, or a bank-certified cashier's check.
- When e-cash created by one bank is accepted by others, reconciliation must occur without any problems.
- Stated, another way, e-cash without proper bank certification carries the risk that when deposited, it might be returned for insufficient funds.
- E-cash must be interoperable-that is, exchangeable as payment for other e-cash, paper cash, goods or services, lines of credit, deposits in banking accounts, bank notes or obligations and for electronic benefits transfers .
- Most e-cash proposals use a single bank.
- In practice, multiple banks are required with an international clearinghouse that handles the exchange-ability issues because all customers are not going to be using the same bank or even be in the same country.
- E-cash must be storable and retrievable.
- Remote storage and retrieval (e.g., from a telephone or personal communications
- device) would allow users to exchange e-cash (e.g., withdraw from and deposit into banking accounts) from home or office or while traveling.
- The cash could be stored on a remote computer's memory, in smart cards, or in other easily transported standard or special purpose devices. Because it might be easy to create counterfeit cash that is stored in a computer, it might be preferable to store cash on a dedicated device that cannot be altered.
- This device should have a suitable interface to facilitate personal authentication using passwords or other means and a display so that the user can view
- the card's contents.
- One example of a device that can store e-cash is the Mondex card-a pocket-sized electronic wallet.
- E-cash should not be easy to copy or tamper with while being exchanged; this includes preventing or detecting duplication and double-spending.
- Counterfeiting poses a particular problem, since a counterfeiter may, in the Internet environment, be anywhere in the world and consequently be difficult to catch without appropriate international agreements.
- Detection is essential in order to audit whether prevention is working. Then there is the tricky issue of double spending. For instance, you could use your e-cash simultaneously to buy something in Japan, India, and England.
- Preventing double spending from occurring is extremely difficult if multiple banks are involved in the transaction.
- For this reason, most systems rely on post-fact detection and punishment. Now we will see the concept of Electronic Cash actually works.

Working of e-Cash
- Electronic cash is based on cryptographic systems called "digital signatures".
- This method involves a pair of numeric keys (very large integers or numbers) that work in tandem: one for locking (or encoding) and the other for unlocking (or decoding).
- Messages encoded with one numeric key can only be decoded with the other numeric key and n one other.
- The encoding key is kept private and the decoding key is made public.
- By supplying all customers (buyers and sellers) with its public key, a bank enables customers to decode any message (or currency) encoded with the bank's private key.
- If decoding by a customer yields a recognizable message;" the customer can be fairly confident that only the bank could have encoded it.
- These digital signatures are as secure as the mathematics involved and have proved over .the past two decades to be more resistant to forgery than handwritten signatures.
- Before e-cash can be used to buy products or ser-vices, it must be procured from a
- currency server.

Purchasing E-cash from Currency Servers
- The purchase of e cash from an on-line currency server (or bank) involves
- two steps (1) Establishment of an account and (2) Maintaining enough money in the
- account to back the purchase.
- Some customers might prefer to purchase e-cash with paper currency, either to maintain anonymity or because they don't have a bank account.
- Currently, in most e-cash trials all customers must have an account with a central on-line bank.
- This is overly restrictive for international use and multicurrency transactions, for customers should be able to access and pay for foreign services as well as local
- services.
- To support this access, e-cash must be available in multiple currencies backed by several banks.
- A service provider in one country could then accept tokens of various currencies from users in many different countries, redeem them with their issuers, and have the funds transferred back to banks in the local country.
- A possible solution is to use an association of digital banks similar to organizations like VISA to serve as a clearinghouse for many credit card issuing banks.
- And finally, consumers use the e-cash software on the computer to generate a random number, which serves as the "note."
- In exchange for money debited from the customer's account, the bank uses its private key to digitally sign the note for the amount requested and transmits the note back to the customer.
- The network currency server, in effect, is issuing a "bank note," with a serial
- number and a dollar amount.
- By digitally signing it, the bank is committing itself to back that note with its face value in real dollars.
- This method of note generation is very secure, as neither the customer (payer) nor the merchant (payee) can counterfeit the bank's digital signature (analogous to the watermark in paper currency).
- Payer and payee can verify that the payment is valid, since each knows the bank's public key.
- The bank is protected against forgery, the payee against the bank's refusal to honor a legitimate note, and the user against false accusations and invasion of privacy.

Digi-Cash (e-Cash):
- Digital forms of value storage or value exchange that have limited convertibility into other forms of value and require intermediaries to convert
- In the case of Digi-Cash, every person using e-cash has an e-cash account at a digital bank (First Digital Bank) on the Internet.
- Using that account, people can withdraw and deposit e-cash.
- When an e-cash withdrawal is made, the PC of the e-cash

user calculates how many digital coins of what denominations are needed to withdraw the requested amount.

- Next, random serial numbers for those coins will be generated and the blinding (random number) factor will be included.
- The ' " result of these calculations will be sent to the digital bank.
- The bank will encode the blinded numbers with its secret key (digital signature) and at the same time debit 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 or she introduced earlier.
- The serial numbers-plus their signatures are now digital coins; their value is guaranteed by the bank.
- Electronic cash can be completely anonymous. Anonymity allows freedom of usage to buy illegal products such as drugs or pornographic material or to buy legal product and services.
- This is accomplished in the following manner. When the e-cash software generates a note, it masks the original number or "blinds" the note using a random number and transmits it to a bank.
- The "blinding" carried out by the customer's software makes it impossible for anyone to link payment to payer.
- Even the bank can't connect the signing with the payment, since the customer's original note number was blinded when it was signed.
- In other words, it is a way of creating anonymous, untraceable currency. What makes it even more interesting is that users can prove unequivocally that they did or did not make a particular payment.
- This allows the bank to sign the "note" without ever actually knowing how the issued currency will be used.
- For those readers who are mathematically inclined, the protocol behind blind signatures is presented.

•Conclusions:

e-Cash Systems are found to be more efficient, which leads have lower prices and lower transaction costs, anybody can use it, as like credit cards, and does not require special authorization. It enhances efficiency in Transactions. Internet transfer of cash is cheap with compare transactions made using credit cards. It can be also be inferred that non-existent of tax trail, in case of money laundering and suspicious forgery accounts.

REFERENCE

1. Analyzing and Managing Banking risk- A Framework for Assessing Corporate Governance and Financial Risk by H.V. Greuning And S.B. Bratanovic, WorldBank | 2. Banking Reforms and Globalisation by Dr. Mohan Prasad S., Dr. Pradeep Kumar. | 3. A Evaluative Study of The Performance of Commercial Banks by D. Sunder Rao | 4. Information Technology Control & Audit by Fadric, Sandro, Daniel, Aurabach Publication | 5. Internet A Nut Shell by Quincie, Orealey Publication | 6. The Global Information Technology Report by Sumitra Dutta, B Lenvin INSEAD | 7. William Stallings: Network security Essential , 2000 | 8. Diana Oblinger: EDUCOUSE, Center for applied research, volume | 2003, March 2003 | |