

Ubiquitous Virtual Currency

¹Shanti Swaroop Moharana, ²T. Seshatalpa Sai, ³Rajadeepan D. Ramesh

¹Dept. of Computer Science BITS Hyderabad

²Dept. of EEE BITS Hyderabad

³Dept. of Computer Science BITS Hyderabad

Abstract: *The whole finance of the world revolves around currency. It may be physical or digital. Currency functions as a unit of account providing a common measure of goods and services being exchanged. The enormous use of paper currency has resulted in deforestation, which is leading to ecological imbalance. For conserving the space, time, and environment there is a need for an alternative currency. In this paper, ubiquitous virtual money is proposed, which is accessible throughout the environment. Ubiquitous currency is a form of electronic money that is spent like pocket change. The transactions can be made secure by the use of biometric identifiers.*

Keywords—*ubiquitous, virtual money, banking, smart money, trackable money.*

I. INTRODUCTION

Money is any physical or virtual object that is exchanged for goods and services. It has a store of value. It functions as a unit of account providing a common measure of goods and services being exchanged. In earlier ages, the exchange of commodity was practiced as barter system. Barter system was generally practiced between complete strangers or potential enemies. It is still used as a method of exchange in times of monetary crisis. Later physical tokens such as gold and silver were used as money.

Fiat money was introduced during Yuan and Ming dynasty in China. Money that derives its value from government regulations is Fiat money. Banknotes and coins are used as currency which comprises the physical aspects of nation's money supply.

With the advent of commercial banks, demand deposits were introduced as claims against financial institutions. Demand deposit withdrawal can be done in person through banks, checks, drafts, ATMS's or through online banking.

Over the years due to increase in population and difference between currency value of various countries, the number of banknotes and coins has immensely increased. Currently over 165,000,000 banknotes and coins are in usage all over the world. For production and printing of banknotes, enormous numbers of trees are being cut down. To maintain the ecological balance we need to find an alternative currency. The world is growing very fast, and everything is moving towards digital from small mobile phone to a complex system such as atomic clocks. For conserving the space, time, and environment, we are proposing a new form of currency named as ubiquitous virtual currency that is not physical and is stored in the cloud. In the present scenario, currency is limited in terms of its reach in monitoring and tracking[1]. This limitation could be eliminated with the advent of ubiquitous currency. Ubiquitous currency is a form of electronic money that is spendable like pocket change. Our proposed ubiquitous currency will evolve from existing technology.

The term ubiquitous computing was coined by Mark Weiser in 1991. Weiser defined ubiquitous computing as the method of enhancing computer use by making many computers available throughout the environment making them effectively invisible. So, we propose a mechanism which makes efficient usage of money by making accessible throughout the environment and hence making it invisible. If we can store, forward and manipulate information similar thing can be done with the money. Now combine this power of money with the fast growing internet. So there is no hindrance in using the concept of ubiquitous money practically.

II. ORGANIZATIONAL STRUCTURE

Our whole proposed system is user centric, and it follows iHCI. On the whole top of the system, there will be centralized financial authority which manages all the states. This group consists of representative from each state. The financial system of every state will be controlled and managed by government authority of that country. The government will identify financial institutions like banks which handles all the transaction of public of that country.

III. REGISTRATION WITH BANKS

Every citizen of a particular country has to mandatorily register with any one of the recognized banks. The registration process involves providing personal details along with biometrics scan. Each registered user will

be provided with a SIM card that has seamless connectivity with bank only. Both will share a common number, and all the transaction will be made on that number. This SIM can be used for transaction of some limited amount. Each SIM will be password protected. The critical limit of the transaction will be limited to 10% of bank account balance. This critical limit can be modified by the user with a password, and the user has to be physically present at the bank for biometric scan. Like the existing bank system for mutual accounts in case of minors, they will be provided with separate SIM. The limit for this separate SIM can be controlled by primary account holder. The critical limit of the transaction is not applicable for minor accounts.

IV. TRANSACTION

The exchange of money is considered as a transaction. It can be in two modes.

- Account holder wants to buy something.
- Account holder wants to transfer money to someone.

All business enterprises like shops, pharmacy, supermarket, hotels, restaurants etc. should have a modular device like biometric scanner. When the customer purchases anything the billed amount is transferred to the business enterprise account.

For transferring money between individuals, account holders can use their mobile SIM[2]. When a user holds his cellphone next to someone else phone, all the devices present in the near field are displayed. Then the user can initiate a transfer process[3]. User can select the payee to whom he wants to transfer money. After selecting the user, the transaction is authorized by the verification password. After verification of the password money will be transferred. If the user wants to transfer a larger amount then it will log a request in the server. After the bank approves the request, money will be transferred. The bank may make a verification call for verifying the log whether it is valid or not.

V. INSTRUMENTING DEVICES

Instrumentation refers to the process of adding sensors, acting as information sources in the physical world. These sources can then be configured and recorded for on-line and of-line analysis. Other systems such as software based system may also be instrumented in order to monitor their operation and to reflect on and even modify their behavior.

A. For Customers

Every user must have a mobile handset. A GSM SIM will be provided by the bank after the registration process is completed.

B. For Banks

- Every bank will have a bio-metric scanner.
- When a registered user enters the bank. A digital token is generated using auto identification through finger print. A message is sent to the customer's mobile number informing the token number, counter number and estimated waiting time. Based on the previous transactions the current preference will be predicted and the particular functionality will be activated.
- When a nonregistered user enters the bank, he will be provided with an interface to enter his mobile number and the purpose of visit. Then a message is sent to the customer's mobile number informing his token number will be generated, and he will be directed towards appropriate counter.

C. Shops

Every shop will have a biometric scanner. All objects in the shop will have a RFID tag which stores information about the object. When the customer puts some item into the digital basket the amount is calculated automatically. During checkout, the biometric scanner will scan the customer and transfer the appropriate amount.

D. Government Organization

- It is the controlling authority which controls the banks.

VI. INTERACTIONS

Interaction is an exchange of information. For the operation of our proposed Ubiquitous money system, interaction is needed. This information is provided by various instrumenting devices. Interaction can be of different types like computer-human, computer-computer, human-human, and human-computer interaction. So we have categorized all the entities into various groups as mentioned in table-1:-

TABLE I. INTERACTION TABLE

| | <i>Government</i> | <i>Bank</i> | <i>Customer</i> | <i>Shop</i> |
|------------|---------------------------|-------------------------------------|---|-------------------------------|
| Government | PC, and Telecom | PC, Telecom, and Legal documents | Circular and Policies | Subsidies |
| Bank | Reports | Customer identification information | Setting critical limit, account modification, and loans | Customer data validation |
| Customer | Tax, Complaints | Registration, and Money Transfer | Money Transfer | Payments |
| Shop | Service tax, Rent and VAT | Transaction confirmation | Digital RFID basket | Whole-sale to retail transfer |

A. Government-Government

All the funds regarding developmental projects like irrigation, agriculture, disaster-relief, education, healthcare, roads etc. and rules-regulations are communicated between governments.

B. Government-Bank

The rules and regulation for banks are provided by the government. These includes loans, interest rates etc.

C. Government-Customer

The government issues various circulars to the customers which includes interest rates, etc.

D. Government-Shops

The government provides a subsidy to customers through shops.

E. Bank-Government

Bank sends various reports to the government. These reports include details of secure transactions like military and suspicious transactions of some customers.

F. Bank-Bank

Bank shares customer identification information with other banks.

G. Bank-Customer

Bank provides various services to the customer. These services include setting critical limit of account, loan, account modifications etc. Bank also provides the facility to transfer large amount of money through biometrics scan.

H. Bank-Shop

Bank provides customer identity validation using biometric scanners.

I. Customer-Government

Customer can lodge a complaint if he is not satisfied with the services of the bank. Customers whose income falls into the category of taxable income must pay their taxes.

J. Customer-Bank

Customer provides his personal details in order to create an account. Customer also pays various bank charges.

K. Customer-Customer

A customer can transfer money to another customer upto the critical limit through the bank given GSM SIM.

L. Customer-Shop

Customer makes payment for the products or articles purchased.

M. Shop-Government

Shops pay taxes applicable to the products.

N. Shop-Bank

Shop provides all the transaction of the customer to the bank.

O. Shop-Customer

Shops will collect data of frequent customers and checks their purchase history. Later it suggests a smart list consisting of frequently purchased items. On selection of an item from a smart list, those articles will be available directly at the counter.

P. Shop-Shop

A wholesale shop can communicate with retail shop if the inventory limit crosses the threshold limit.

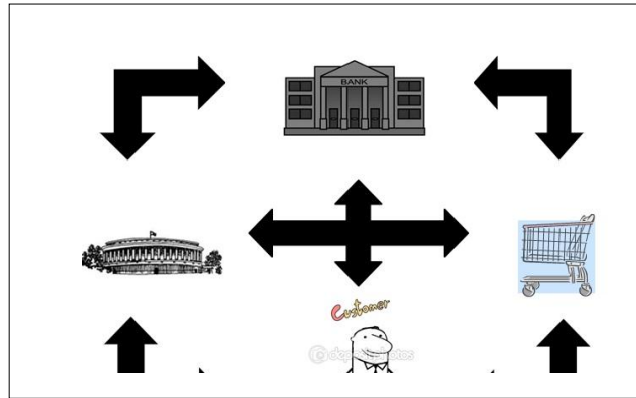


Fig. 1. Interaction diagram

VII. TECHNOLOGIES USED

A. BIO-METRIC:

Bio metrics refers to the identification of humans by their characteristics traits. It can be used for identification and access control. Bio metric identifiers are the distinctive measurable characteristics used to label and describe individuals. Since bio metric identifiers are unique to individuals they are more reliable in verifying identity than token and knowledge-based methods. A bio metric system can operate in two modes. In verification mode, the system performs a one to one comparison of a captured bio metric with a specific template stored in a bio metric database in order to verify the individual. In identification mode the system performs one to more comparison against a biometric database in an attempt to establish the identity of an individual. The first time an individual uses a biometric system is called enrollment. Moreover, biometrics is one of the few techniques that can be used for negative recognition where the system determines whether the person is who denies being.

B. GSM:

The GSM standard was developed as a replacement for first generation analog cellular networks. It is a digital circuit switched network which is optimized for full duplex voice telephony. Over the years, data communication was included in GSM. Phase 1 of the GSM specification was published in 1990. It refers to the global system for mobile which is a cellular technology that is used to transfer mobile, voice, and data services. It is the most widely spread cell technology throughout the world. It provides a more stable network with robust features. It has less signal deterioration inside buildings. GSM provides anonymity[4],[5] which blocks one user from accessing the other user's system without his consent. It provides secure data transfer through the use of encryption. It enables seamless interoperability between networks.

C. RFID:

Radio frequency identifier tags can be attached to objects to enable their identification in the world over a wireless link. It does not require a line of sight, and manual orientation to read the tag. RFID can be classified into active tags and passive tags. Active RFID tags have their own energy supply while passive RFID tags use energy supply of the reader. Active RFID tags are used on large assets such as a cargo container, rail-cars and large re-usable containers that need to be tracked over distances. Active RFID tags operate at 450MHz, 2.45 GHz or 5.8 GHz frequency and have a read range of 2200 meters. Passive RFID tags contain no power source and no active transmitter. Passive RFID tags operate at low frequency 125-135 KHz, high frequency 13.56 MHz and Ultra high frequency 860-960MHz.

VIII. OPERATIONAL CHALLENGES

A. SECURITY

Bio-metric information cannot be acquired just by simple observation. It is impossible to share and difficult to reproduce. It enhances user convenience by alleviating the need to memorize long and random password. It provides the same level of security to all users, unlike passwords and is highly resistant to brute force attack.

B. PRIVACY

Consider a scenario in a shop where a person has to provide bio-metric details in order to pay for the things purchased. There is a possibility that the data obtained during the transaction may be used in incorrect

ways by the shopkeeper. This can be restricted by providing only necessary details to the shopkeeper. Any agency that wishes to access any individual's transaction need to get permission from the concerned authority.

IX. CONCLUSION

In this paper, we have discussed the idea, design and technology of a world without paper currency. We have described the interaction involved in the system between different entities. We have proposed different technologies involved in the interaction between entities. The idea is to use the existing GSM technology for making the money ubiquitous. This makes the money accessible throughout the environment and hence making it invisible. By removing the physical currency, we are making it trackable. This whole process is made secure using biometric identifier. We have used bio metric identifiers as it can be used to identify the individual uniquely. Hence it is more reliable in verifying identity than token and knowledge-based methods. System is designed in such a way that it protects the privacy of the user.

REFERENCES

- [1] Manikandan, Madhusudhanan. J, Dr. Prasanna Venkatesan.V, Amrith.V, Martial Arokiadoss Britto "Smart Banking Environment based on context history" IEEE- International Conference on Recent Trends in Information Technology, ICRTIT 2011
- [2] Mohammed A. Qadeer, Nadeem Akhtar, Shalini Govil, Anuja Varshney "A novel scheme for mobile payment using RFID-enabled Smart SIM card" International Conference on Future Computer and communication 2009
- [3] Abdullahi Arabo "Secure Cash withdrawal through Mobile phone/Device " Proceedings of International Conference on Computer and communication engineering 2008
- [4] Vishwas Patil and R.K.Shyamasundar "An efficient, secure and delegable Micro-Payment System " IEEE.
- [5] Gianluigi Me and Maurizio Adriano Strangio "Mobile local macro-payments:security and prototyping" IEEE CS and IEEE ComSoc.