Official Digital Currency

M. Shoaib
International Islamic University,
Islamabad, Pakistan
shoaibishaaqiiu@yahoo.com

M. Ilyas
International Islamic University,
Islamabad, Pakistan
mhdilyas@hotmail.com

M. Sikandar Hayat Khiyal
Army Public College of
Management and Sciences
Rawalpindi, Pakistan
m.sikandarhayat@yahoo.com

***Abstract*—In ancient times goods and services were exchanged through barter system[1]. Gold, valuable metals and other tangibles like stones and shells were also exploited as medium of exchange. Now Paper Currency (PC) is country-wide accepted common medium of trade. It has three major flaws. *First*, the holder of currency is always at risk due to theft and robbery culture in most of the societies of world. *Second*, counterfeit[2] currency is a challenge for currency issuing authorities. *Third*, printing and transferring PC causes a heavy cost. Different organizations have introduced and implemented digital currency systems but none of them is governed by any government. In this paper we introduce Official Digital Currency System (ODCS). Our proposed digital currency is issued and controlled by the state/central bank of a country that is why we name it Official Digital Currency (ODC). The process of issuing ODC is almost same as that of Conventional Paper Currency (CPC) but controlling system is different. The proposal also explains country-wide process of day to day transactions in trade through ODCS. ODC is more secure, reliable, economical and easy to use. Here we introduce just the idea and compulsory modules of ODC system and not the implementable framework. We will present the implementable framework in a separate forthcoming publication.**

Keywords

Paper currency, digital currency, virtual currency, number currency, e-currency, currency systems

I. Introduction

A. *History of Currency*

Payments were being made as early as 2200 BC using some form of currency [1]. In ancient times goods and services were exchanged for goods and services called barter system of trade. The co-incidence of availability of goods and services and wants between the parties was a bottleneck for trade. Gold, valuable metals and tangibles like stones and shells have also been exploited for long as means of exchanging goods and services.

Gold certificates (an example of commodity-backed money) were exchanged for a fixed quantity of fundamental commodity [1]. Ease of portability was main advantage of this currency. Now-a-days Paper Currency is country-wide accepted common medium of trade. Every country has its own paper currency exchangeable by other currencies of the world at an arbitrary rate.

B. *Functions of Money*

Regardless of the nature of money, it has three different functions:

- *Medium of exchange*: it is medium of exchange to avoid inconveniences of a barter system. It fulfills the need for a coincidence of wants of the parties involved in transactions.
- *Unit of account*: it is a standard numerical unit for the measurement of value of goods and services.
- *Store of value*: it can be stored and reused in future.

Paper currency has three major flaws. *First*, the holder of currency is always at risk due to poor enforcement of law and order in the society. There are millions of robbery cases in which currency holders are gunned down. *Second*, counterfeit currency is severe headache for currency issuing authorities. Weaker the government, there are more chances of counterfeit currency. No country can claim that all her currency notes circulating throughout the world are genuine. Counterfeit currency is one of the causes of devaluation of currency and inflation in the country. *Third*, printing and transferring PC causes heavy cost. In Pakistan all branches of a bank are bound by law to deposit all the collected money at nearby head branches at day end. At beginning of next day reasonable amount is again sent back to the branches. This is an example of costs occurring on transporting the currency. Individual people also spend heavy amount to secure their paper money.

Rest of the paper is organized as follows. Section II discusses the related work of DC. Section III explains the ODC system. Section IV describes the process of transferring money through ODCS. Section V and VI are reserved for advantages and issues of ODCS. Section VII investigates the deployment feasibility of our proposed ODCS. Section VIII provides summary and future directions of this work.

[1] System of trade in which goods and services were exchanged for goods and services.

[2] Counterfeit currency (fake currency) is imitation currency produced without the legal sanction of the state or government.

978-1-4799-0615-4/13/$31.00 ©2013 IEEE

II. Related Work

In spite of many days' searching we could not find any literature about any form of digital currency issued and controlled by government. However closely relevant concepts have much material on Internet. Virtual currency/money, e-cash [2][3], cyber-cash, etc are all digital currencies. The authors of [1] define virtual currency as: "*a virtual currency can be defined as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community*". Bitcoin [1] [4][5][6], Litecoin [2] and Novacoin [3] are examples of digital currencies. Different organizations have introduced and implemented digital or virtual currency systems but none of them is governed by any government [1]. Initially virtual currencies were used for virtual goods on Internet like online games. Now they are also used in transactions with real goods and services and are not limited to online games. Many digital currencies are backed by a guarantee to pay some gold or silver bullion in exchanging each of its units[1]. Others are float depending upon the willingness of individuals [1]. References [7][8][9] and [10] describe different aspects of virtual currencies.

Works in this area are not limited to few schemes. There are dozens of digital currency systems spanning from e-cash [2] [12][13][14][15], to trusted intermediaries [16][17][18]. In these systems spending money is easy as members are willing to accept any valid bill. All these currencies systems are decentralized. The structures upon which these systems are built are not well-suited with the goals of decentralized systems. They necessitate a central authority to issue and control digital currency.

Digital or virtual currencies have many flaws. For example, they do not tend to be inherently stable, could have a negative impact on the reputation of central banks, and are not issued and controlled by any powerful authority [1]. Much detail on virtual currencies is available in [1]. Reference [11] describes in detail that virtual currencies are not real currencies. We focus our attention to our proposed official digital currency.

In this paper we introduce implementable official digital currency system at larger scale, i.e., at state level. The official digital currency is issued and controlled by the central/state bank of the country. The process of issuing the ODC is almost same as that of conventional paper currency but the controlling system is different. In next sections we explain the system for issuing, distributing and controlling ODC. This paper also explains the country-wide process of day to day transactions in trade for local consumers (all citizens of a country). World-wide process of payments through ODC will be explained in separate forthcoming publication. Our proposed ODC is more secure, reliable, economical and easy to use.

A. Defining Official Digital Currency

We define official digital currency as "*the system generated sequential numbers issued by state/central bank and replaceable by conventional paper currency*". Here "replaceable" we mean that a note of ODC can be exchanged with a note of paper currency of the same value at equal rate as both are issued by the same authority. Similarly a note of PC is exchangeable with that of ODC.

ODC is nothing except numbers, so we can call this currency as number currency too. CPC is also nothing except numbers. In Pakistan, we can replace our damaged paper currency note from the State Bank of Pakistan (SBP) if we have preserved its number. The state bank destroys that note and prints a new one bearing the same number and value.

B. Our Contribution

In this paper we present an innovative idea of official digital currency. The proposed system of ODC can replace conventional paper currency system at large resolving major issues of paper currency discussed above.

C. Difference between Present Digital Currencies and ODC

Here we highlight four major differences: (1) ODC is issued and governed by the currency issuing authority of the country whereas same is not true for conventional digital currencies. (2) No digital currency coin is replaceable by any official currency note whereas ODC notes are replaceable by official PC notes at equal rate. (3) The exchange rate of ODC against other valid currencies of the world is exactly same as that of official PC but the case of conventional digital currencies is different. (4) Conventional digital currencies are mostly in action in closed communities on Internet. The ODC is designed for all the users of paper currency.

III. ODC System

In this section we explain our proposed Official Digital Currency System (ODCS).

[1] http://bitcoin.org/en/

[2] http://Litecoin.org/

[3] https://bitcointalk.org/index.php?topic=143221.0

A. Users of ODCS

Any of the users of paper currency may become the user of ODCS. Business organizations, governmental departments and financial institutions are important users of ODCS. Individual persons may also become users of this system. There is no restriction to become the user of ODCS except to have an account in any bank.

B. Modules of ODCS

Figure 1 visualizes main modules of ODCS. Here we describe briefly functions of the modules of ODCS. Technical discussion of these modules is postponed to a forthcoming article.

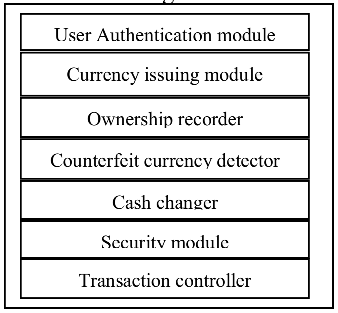

Figure 1: Modules of ODCS

i User Authentication Module

This module is observed in all types of secured systems. This module confirms the registered user and his/her authority. Different types of users have different privileges. For example, issuing ODC notes is authorized only with the state/central bank.

ii Issuing ODC Module

In Pakistan, State Bank of Pakistan (SBP) is authorized to issue CPC notes. Our proposed ODC is replaceable by paper currency so the SBP should have authority to issue ODC on behalf of government of Pakistan. For this purpose state bank neither needs papers nor printing infrastructure. Only the creation of sequential numbers by computer is required. Each number is actually the Digital Currency Note (DCN) replaceable by CPC note. Different series of numbers can be assigned to DCNs having specific value. This is nothing new; the CPC notes are also issued on the same principal. For example a Rs. 500 note has number 'BU1964521' and a Rs. 20 note 'C1263636' (see figure 2(a)). Here 500 and 20 are values and BU1964521 and C1263636 are serial numbers of notes. Surely theses two numbers belong to two different series. Multiple series of numbers can be exploited for the same value notes whenever needed.

In Pakistan, at present paper notes of seven different values (5000, 1000, 500, 100, 50, 20 and 10) and coins of three different values (5, 2 and 1) are issued by the SBP and government of Pakistan. The matter of coins is different from that of paper notes as the former do not bear any number. Figure 2(b) shows images of different currency notes and coins issued by the central authority. What is the most important thing in PC notes? Surely it is their serial number. If this number is not readable the note goes waste. The coins can also be replaced with ODC notes/coins if assigned serial numbers.

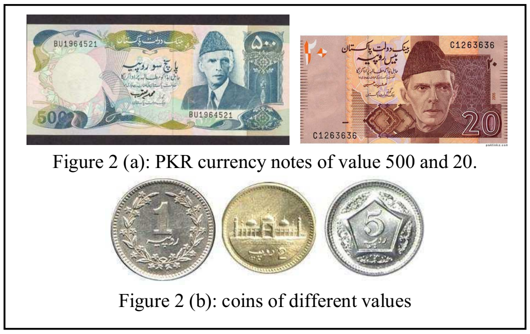

Figure 2 (a): PKR currency notes of value 500 and 20.

Figure 2 (b): coins of different values

Figure 2: Pakistani currency notes of Rs. 500 and 20, and coins of Rs. 1, 2 and 5.

In our proposed ODC we exploit only the serial numbers. For example a series from AA0000000 to AA9999999 can be generated representing the ODC notes of value Rs. 1000 each. In this way 10^7 digital notes can be issued having the total worth 10^{10} Pakistani rupees. Similarly different series of numbers can be generated for digital notes of different values. In ODC we need not to store the images of each currency note. Although, technically it is possible but it is mere wastage of storage space in computers and it will be a great barrier to perform efficient transactions in real life.

Issuing numbers representing currency notes is very simple but securing money in this system is not as easy as its creation. We need to make our system as secure as possible. ODCS is not acceptable for any government if it is unsecure. We will discuss the security of the system in a separate article.

iii Ownership Recorder

Recording the ownership is recommended in ODCS. The ownership of Official Digital Currency Notes (ODCNs) is recorded by ODCS for each ODCN or series of ODCNs. That means ODCS knows the owner of ODC notes. In this case the account numbers in different banks represent the owners ID. That means the account holders are owners of money. The ownership ID of each department, financial institution, organization, individual persons may be represented through bank accounts or any other feasible identifier. The commercial banks may facilitate the individual persons who don't have proper accounts by opening new accounts as required by the ODCS and SB.

iv Counterfeit Currency Detector

Recording the number of each ODCN involves complexity especially in business transactions. Why do we record the number of each ODCN? The basic purpose is to avoid counterfeit notes of ODC. The originality of each ODC note can be investigated by the SB or any other bank (if authorized) simply by two checks. (1) Was a number (note) under discussion generated by the SB? (2) Does any other account owns the same number? If the answer to the first question is "no" that means the note is surely counterfeit. If the answer to the first question is "yes" then second check is needed to be investigated. The answer "no" to the second question guarantees that the note is not counterfeit. Else the counterfeit note has entered the system. If multiple copies of the same number (note) are identified then it is responsibility of this module to investigate which account has the genuine number (note). Counterfeit copies of the number (note) are destroyed and the concerned account holder and commercial bank may be informed to back track the counterfeit note transactions to find the reason of the counterfeit note in the system.

v Cash Changer

Buyer's account may have reasonable amount for accomplishment of the transaction but it is quite possible that the account has bigger notes making the transaction impossible to transfer the exact amount. For example, Buyer's account has 100 ODC notes each amounting Rs. 1,000. The amount to be transferred is Rs. 55,200. In this scenario cash changer module helps the buyer by providing 10 ODCNs of Rs. 100 each, in exchange of 1 ODCN of Rs. 1000. This module does not need to get permission from the account holder to perform this function.

vi Security Module

Securing ODCS from cyber attacks is the only key issue of this system. If we are able to provide fool proof security to our proposed ODCS, there is no other hurdle that can restrict its deployment. We are working on this module and it will be introduced in a separate paper.

vii Transaction Controller

We describe the process of the transaction controller in next section. Here, we are concerned only with the transfer of ODCNs from one account to the other along with the necessary functions required by ODCS (like recording ownership, detecting counterfeit currency, providing change for bigger notes, etc.). The complete process of transactions is the responsibility of commercial banks.

IV. Transferring Money

A. *Transferring Money between State Bank and other Banks*

ODC can be easily transferred from SB to account heads of different departments in different commercial banks. What is transferred? Only the numbers are transferred. Here we explain the process of transferring 10^7 ODC notes having total worth 10^{10} Pakistani rupees (each note having value Rs. 1000). Suppose there are 10 departments and each department has equal share. The digital notes from numbers AA0000000 to AA0999999 having total worth 10^9 rupees are transferred to department 1, AA1000000 to AA1999999 to department 2 and so on.

B. *Transferring Money among the Financial Institutions*

The financial institutions are responsible for keeping records of each transaction. What should be recorded along with each transaction? The number (like BU1964521) of each ODCN used in transaction and the new owner (definitely that is account number of another institution) must be recorded. The value of ODCNs against each number and the total amount may be recorded for each transaction.

C. *Transferring Money in Day to Day Business Transactions*

This is the most critical area of our proposed ODCS. When a transaction is committed new ownership of each ODCN used in transaction must be recorded by the ODCS. Our proposed ODCS is not responsible for business rules and requirements of commercial banks. ODCS is only concerned to its modules discussed above. (For simplicity we assume that there are only two parties in a transaction (the seller and the purchaser of goods or services)).

While thinking about such transactions many questions come to mind. Who will tell the system to transfer ODCNs of this and this number? Will all the ODCNs of same value in an account bear consecutive numbers? What is solution if the buyer needs a change for bigger ODCN? Does the user of ODC need to remember numbers and values of all ODCNs? Answer to the first question is "ODCS". The ODCS has a fully automated module that decides at run time which notes (numbers) to be transferred to the seller's account. No human interaction is needed here. The answer of the second question is 'no' because an account is normally credited through different resources (accounts). The answer to the third question is again “ODCS”. The ODCS arranges smaller units of ODCNs whenever needed by the system. It is done by a fully automated module. The buyer’s bank is responsible for providing the smaller units at runtime without involving the account holder (buyer). The bank may accomplish such requests by using a Cash Change Auxiliary account specially created for this purpose. Through this process the ownership is recorded for each ODCN that is transferred. The answer to the last question is “no”. It is the responsibility of the ownership module of ODCS.

V. Advantages of ODCS

The ODC has following advantages over CPC.

- Counterfeit currency is severe headache for currency issuing authorities. Weaker the government, there are more chances of counterfeit currency. No country can claim that all her currency notes circulating throughout the world are genuine. Counterfeit currency causes many problems in the society; devaluation and inflation are important issues. ODCS assures to prevent the circulation of counterfeit currency in the country. The authentication of the number reserved for the ODCN is a good tool for checking counterfeit currency. Duplication of a number can be easily detected by ODCS system. Counterfeit currency, if appeared, can be successfully detected by the system. In CPC system the lay man is not sure about the originality of the currency notes in hand, and even the machines sometimes fail to detect counterfeit currency.
- Holder of paper currency is always at risk due to poor enforcement of law and order in most of the societies. There are millions of robbery cases in which the currency holders are gunned down. The risk of robbery is minimized and even if a robber gets transferred some amount on gun point, or any fraudulent through fraudulent means it can easily be tracked through ownership of the ODCNs.
- Cost occurring on issuing ODC is negligible small. The governments spend a lot of money on printing currency notes. Pakistani government has stopped printing currency notes of Rs. 1, 2 and 5 due to heavy expenses incurred on their printing and reprinting of damaged ones.
- Cost of transferring money in ODCS is also less than that of CPC system. Transferring the CPC physically causes a heavy cost. In Pakistan all the branches of a bank are bound by law to deposit all the collected money at nearby head branches at day end. At next day start reasonable amount is again sent back to the branches. This is an example of cost occurring on transporting the currency. Individual people also spent heavy amounts to secure their paper money while physically transferring from one place to another.
- The cost of securing money in ODCS is also less than that of CPC system. Security is a great issue and causes heavy costs not only in developing countries but also in many advanced countries the situation is not far different. In Pakistan all financial institutions employ a team of security guards to guard the paper money. Instead expending heavy amounts on security. The ODCS guaranties to secure the digital money only by securing the system from hackers. If any robber forces a person at gun point to transfer money to his/her account, it will be easy job for ODCS to detect the culprit.
- There is no issue of smaller units of money in business transactions. In CPC system sometime a business transaction, at retail shops, is not possible due to unavailability of change for bigger notes.
- In CPC system sometimes sellers do not accept smaller units of money from the buyer if the transaction involves a heavy amount. This problem is easily resolved by the ODCS as the buyer’s bank is always ready to help its account holders through Cash Change Auxiliary Account.

VI. Issues in ODC

ODC has some issues that are not faced by CPC.

- It cannot replace CPC completely in near future. Presence of CPC parallel to ODC is must. CPC alone is working properly but ODC alone may not. In far future ODC alone may replace the CPC completely.
- Securing the ODCS from cyber attacks is not an easy task.
- Transactions may be affected in case of technology failure. During war the ODCS infrastructure may be affected adversely.

In spite of these issues the ODCS is worthwhile to be deployed as the advantages are manifold to the disadvantages.

VII. Deployment Feasibility

The ODCS requires a computer or cell phone and VPN or the Internet. A little educated person after short training can make transactions on ODCS. We recommend deploying ODCS parallel to the CPC system. No user is bound to make transactions through ODCS. Every citizen may own ODC or PC or both. The adoptability of ODCS will be faster in advanced countries and slower in developing countries because of low literacy rate and lacking of information technology infrastructure.

Why CPC is needed in presence of ODC?

Initially people will avoid making transactions through ODCS because:

- The transactions may involve very little amounts. For example, transactions at school tuck shop.
- The purchaser may be an uneducated/unskilled[1] person or a child or even a kid.
- The seller or purchaser may not have bank account.
- The ODCS infrastructure may cause any problem at any time (for example no signals of cell phone).
- The purchaser has zero balance of ODC but may have CPC in hand.

Ignoring the above scenarios the business transactions can be easily made through ODCS. All parties involved in a transaction (the sellers and purchasers) must have created their account in the ODCS (this may be their old bank account).

VIII. Conclusion and Future Work

We have introduced the idea o f official digital currency issued and controlled by the state/central bank. The financial institutions are responsible to maintain the accounts of the citizens for this purpose. These institutions play active role in each transaction involving ODC. The ODC is nothing except system generated numbers. Each number represents a virtual note of a specific value. The virtual notes are replaceable by the CPC notes. The ODC has three major advantages over the CPC. It assures prevent the circulation of counterfeit currency in the country. The risk of robbery is minimized and even if a robber gets transferred some amount on gun point or through fraudulent means it can easily be tracked through ownership of the virtual currency notes. The cost occurring on issuing currency is negligible small and the cost of transferring and securing money in ODCS is also less than that of CPC's system. Little educated person after short training can easily use the ODCS easily. This system does not require any additional devices. Only the computer or cell phone connected to the Internet is required to perform the transactions. Initially small portion of public seems to be agreed to use this system but with the emergence of ODC people will prefer to make transactions through ODCS especially for the huge amount transactions. We do not recommend use this system at busy sale points involving very small amounts like school tuck shops etc. For future work we are working on implementable framework of ODCS. This framework ideally should elaborate technical discussion of all the modules of ODCS. The security issues that may be bottleneck of the ODCS is an interesting area for future work. We are also working on the international payment process through ODCS.

IX. Acknowledgement

This research work is possible due to the financial assistant of Higher Education Commission of Pakistan through indigenous 5000 PhD fellowship program. Without the financial assistant of HEC it would have not been possible.

REFERENCES

[1] European Central Bank (2012), "Virtual currency scheme", *a report*.

[2] H. V. Antwerpen, (1990), "Electronic cash", *Master's thesis, CWI*, Netherlands.

[3] C. Lim and P. Lee (1993), "A practical electronic cash system for smart cards", In *Workshop on Information Security and Cryptography*, Korea-Japan.

[4] B. James (2011), "Bitcoins: What are they, and how do they work?", *The Guardian*, 22 June.

[5] C. Stephen (2011), "Bitcoin: A guide to the future of currency", *ZDNet*, 15 June.

[6] Grinber and Reuben (2011), "Bitcoin: An innovative alternative digital currency", *Yale Law School Working Paper Series,* April.

[7] G. Jingzhi and C. Angelina (2008), "Virtual money systems: a phenomenal analysis", Proceedings of the *10th IEEE Conference on E-Commerce Technology* and the *Fifth IEEE Conference on Enterprise Computing, E-Commerce and E-Services*, 21-24 July, pp. 267-272.

[8] G. Jingzhi, C. Angelina and G. Zhinguo (2009), "Virtual wealth realization in virtual and real worlds", Proceedings of the *IEEE International Conference on e-Business Engineering*, 21-23 October, pp. 85-94.

[9] L. V. Orman (2010), "Virtual money in electronic markets and communities", *Johnson School Research Paper Series*, No 27.

[10] P. Hui and S. Yanli (2009), "The theoretic and empirical analysis on the impact of network virtual money on real money supply", Proceedings of the *International Conference on Future Computer and Communication*, Kuala Lumpar, 3-5 April.

[11] W. Ivan (2009), "Why a virtual currency is not a currency?" available at *http://www.ivanwalsh.com/technical-writing-tips-tools/why-a-virtual-currency-is-not-a-currency*

[12] T. Eng and T. Okamoto (1994), "Single-term divisible electronic coins", In *Eurocrypt*.

[13] R. Hirschfeld (1992), "Making electronic refunds safer", In *Crypto*.

[14] T. Okamoto and K. Ohta (1991), "Universal electronic cash", In *Crypto*.

[15] H. Youm, S. Lee, and M. Rhee (1993), "Practical protocols for electronic cash", In *Workshop on Information Security and Cryptography*, Korea-Japan.

[16] F. D. Garcia and J. H Hoepman (2005) "Off-line

[1] Unskilled means that he/she is unaware of using ODCS

karma: A decentralized currency for static peer-to-peer and grid networks". Proceedings of *International Networking Conference (INC)*.

[17] V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer (2003), "KARMA a secure economic framework for p2p resource sharing", In *P2PEcon.*

[18] N. Tran, J. Li and L. Subramanian (2010) "Collusion-resilient credit based reputations for peer-to-peer content distribution", In *NetEco.*