Official Digital Currency: The Future Currency

Muhammad Shoaib[1], Muhammad Ilyas[1], Malik Sikandar Hayat Khyial[2]
[1]Faculty of Basic and Applied Sciences
International Islamic University
[2]Faculty of Computer Sciences
Preston University
Islamabad, Pakistan
{shoaibishaaqiiu, m.sikandarhayat}@yahoo.com, mhdilyas@hotmail.com

ABSTRACT: *In earlier days of humanity when there was no currency goods and services were exchanged through barter system[1]. Gold and other valuable metals were also exploited as medium of exchange. With the invent of paper currency (PC) trade transactions became very easy. In spite of its advantages paper currency has three major flaws: first, the holder of currency is always at risk due to lawlessness culture in many societies of the world. Second, counterfeit currency is a big issue for governments and currency issuing authorities. Third, printing and transferring PC causes heavy costs. Private organizations have introduced digital currencies like bitcoin[2] but none of them is guaranteed or governed by any government. That is why they are used in a closed environment against particular commodities. In this paper we introduce implementable digital currency system at larger scale, i.e., at state level. Our proposed digital currency is issued and controlled by the state or central bank of the country and we name it official digital currency (ODC). The process of issuing ODC is almost same as that of conventional paper currency (CPC) but the controlling system is different. ODC coins or notes are digitally produced hence eliminate the need for any metal or paper. Here we propose the system for issuing, distributing and controlling ODC. The proposal also explains the country-wide process of day to day transactions in trade through ODC. Our proposed currency aims to be the real currency at macro and micro levels. The ODC is more secure, reliable, economical and easy to use. In this paper 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 publication.*

Keywords: Paper Currency, Digital Currency, Virtual Currency, Number Currency, E-currency, Currency Systems

Received: 28 July 2013, Revised 30 July 2013, Accepted 4 August 2013

1. Introduction

1.1 History of Currency

The Payments were being made as early as 2200 BC using some form of currency [1]. In ancient times goods and services were

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

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

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 and other valuable metals 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 the fundamental commodity. Ease of portability was main advantage of this currency. Today's economies are based on paper currency which is the biggest and world-wide accepted medium of exchange. Every country has its own paper currency.

1.2 Functions of Money

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

- **Medium of exchange**: It is the medium of exchange to avoid the 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. The counterfeit currency causes 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 next day start 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.

Different organizations have introduced and implemented digital or virtual currency systems but none of them is governed by any government [1]. 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[3] [2] [3] [4], Litcoin[4] and Novacoin[5] are examples of digital currencies. Initially virtual currencies were used virtual goods on Internet. Now digital currencies 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. Others are float depending upon the willingness of individuals. References [5] [6] [7] and [8] describe different aspects of virtual currencies.

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. The major flaw of these currencies is that they are not issued and controlled by any government agency. Much detail on virtual currencies is available in [1]. Reference [9] 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 the country). World-wide process of payments through ODC will be explained in separate publication. Our proposed ODC is more secure, reliable, economical and easy to use.

1.3 Official Digital Currency

We define official digital currency as "*the system generated sequential numbers issued by state/central bank and replaceable*

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

[4] http://litecoin.org/

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

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 as both are issued by the same authority. Similarly a note of PC is exchangeable with that of DC.

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.

1.4 Our contribution

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

1.5 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 is replaceable by any official currency whereas ODC is replaceable by the official PC. The exchange rate of ODC against other valid currencies is exactly same as that of official PC. Same is true for day to day transactions involving goods and services. (4) Conventional digital currencies are mostly in action in closed communities on Internet. The ODC is designed for all the users of paper currency.

2. ODC System

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

2.1 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 the users of this system. There is no restriction to become the user of ODCS except to have an account in any bank.

2.2 Modules of ODCS

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

2.2.1 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.

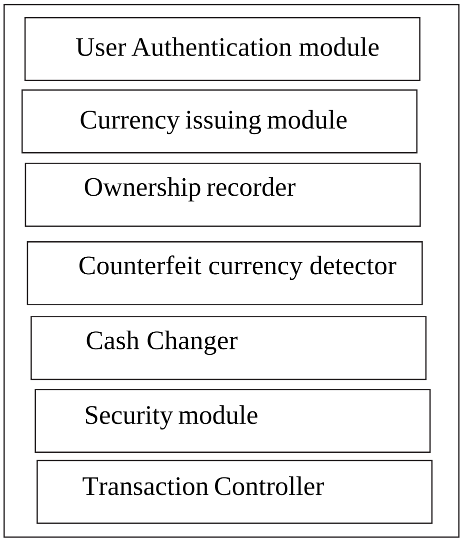

Figure 1. Modules of ODCS

2.2.2 Issuing ODC Module

In Pakistan, the state bank of Pakistan 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 the government of Pakistan. For this purpose the state bank neither needs papers nor the printing infrastructure. Only the creation of sequential numbers by the 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 the values and BU1964521 and C1263636 are the serial numbers of the 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 six different values (1000, 500, 100, 50, 20 and 10) and coins of three different values (5, 2 and 1) are issued by the SBP. 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 SBP. 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 DC notes. ODCS needs not to have coins along with notes.

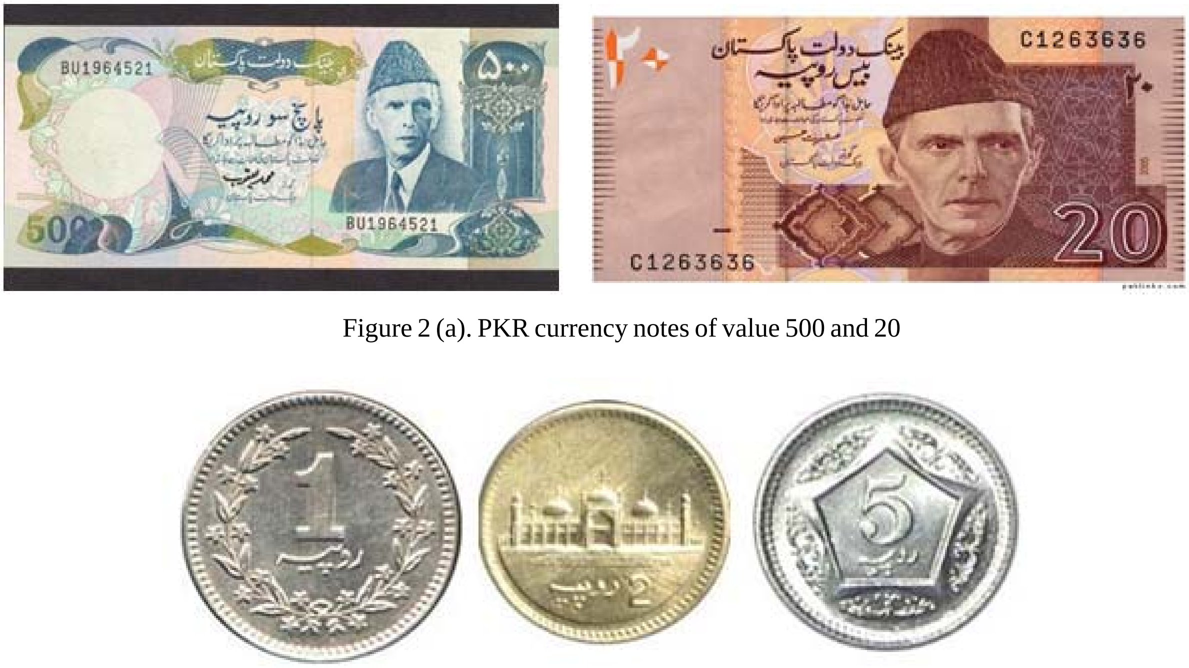

Figure 2 (a). PKR currency notes of value 500 and 20

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 107 digital notes can be issued having the total worth 1010 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 the numbers representing currency notes is very simple but securing the 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.

2.2.3 Ownership Recorder

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

2.2.4 Counterfeit Currency Detector

Recording the number of each DCN involves much more complexity especially in business transactions. Why do we record the number of each DCN? The basic purpose is to avoid counterfeit notes of ODC. The originality of each DC note can be investigated by the SB or any other bank (if authorized) simply by two checks. Was a number (note) under discussion generated by the SB? Does any other account own 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.

2.2.5 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 DC notes each amounting Rs. 1,000. The amount to be transferred is Rs. 55,200. In this scenario the cash changer module helps the buyer by providing 10 DCNs of Rs. 100 each in exchange of 1 DCN of Rs. 1000. This module does not need to get permission from the account holder to perform this function.

2.2.6 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.

2.2.7 Transaction Controller

We describe the process of the transaction controller in next section. We are concerned only with the transfer of DCNs 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.

3. Transferring Money

3.1 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 107 DC notes having total worth 1010 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 109 rupees are transferred to department 1, AA1000000 to AA1999999 to department 2 and so on.

3.2 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 DCN used in transaction and the new owner (definitely that is account number of another institution) must be recorded. The number of DCNs against each value and the total amount may be recorded for each transaction.

3.3 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 DCN 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 DCNs of this and this number? Will all the DCNs of same value in an account bear consecutive numbers? What is solution if the buyer needs a change for bigger DCN? Does the user of ODC need to remember numbers and values of all DCNs? 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 ODC 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 an auxiliary account specially created for this purpose. Through this process the ownership is recorded for each DCN transferred. The answer to the last question is "*no*". It is the responsibility of the ownership module of ODCS.

4. 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, inflation is one of them. ODCS assures to prevent the circulation of counterfeit currency in the country. The authentication of the number reserved for the DCN 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 virtual currency notes.

- 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 there are hundreds of bank robbery cases. Individual people also spent heavy amounts to secure their paper money. Thousands of people have been killed by robbers during robbery. 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 is smaller units of money in business transactions. In CPC system sometime a business transaction is not possible due to unavailability of change.

- 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.

5. Issues in ODC

The ODC has some issues that are not faced by the CPC.

- It cannot replace the CPC completely in near future. The 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.
- It is IT dependent; 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.

6. 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.

Why CPC is needed in presence of ODC?

Initially people will avoid making transactions through ODCS.

- 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 created his/her account in ODCS.
- The ODCS infrastructure may cause any problem (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 the parties involved in the transaction (the sellers and purchasers) must have created their account in the ODCS (this may be their old bank account).

7. Acknowledgement

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

8. 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 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 the security issues that may be bottleneck of the ODCS. After achieving high level of security the ODCS will be ready for local transactions. We are also working on the international payment process through ODCS. After completing this module ODCS will be ready for world-wide transactions.

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

References

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

[2] BALL, James. (2011). Bitcoins: What are they, and how do they work?, The Guardian, 22, June.

[3] CHAPMAN, Stephen. (2011). Bitcoin: A guide to the future of currency, ZDNet, 15, June.

[4] GRINBERG, Reuben. (2011). Bitcoin: An Innovative Alternative Digital Currency, Yale Law School Working Paper Series, April.

[5] GUO, Jingzhi, CHOW Angelina. (2008). Virtual Money Systems: A Phenomenal Analysis, *In*: Proceedings of the 2008 10th IEEE Conference on E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing, E-Commerce and E-Services, 21-24 July, p. 267-272.

[6] GUO, Jingzhi, CHOW, Angelina, GONG, Zhinguo. (2009). Virtual Wealth Realization in Virtual and Real Worlds, IEEE International Conference on e-Business Engineering, 21-23 October, p. 85-94.

[7] ORMAN, Levent, V. (2010). Virtual Money in Electronic Markets and Communities, Johnson School Research Paper Series, No 27.

[8] PENG, Hui, SUN, Yanli. (2009).The theoretic and empirical analysis on the impact of network virtual money on real money supply, International Conference on Future Computer and Communication, Kuala Lumpar, p. 3-5 April.

[9] WALSH, 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.