A Study of CBDC Model Applicable for the Current Banking Environment

Sajan Maharjan, KyungChan Ko, ChangHoon Kang, JongSoo Woo, James Won-Ki Hong

Department of Computer Science and Engineering, POSTECH
{thesajan, kkc90, chkang, woojs, jwkhong}@postech.ac.kr

Abstract

The emergence of blockchain and cryptocurrency technology has induced significant impact on the financial services area. Governments and banks are keen to utilize this novel technology for their benefits of cost reduction, greater transparency and control. This has resulted in the concept of central bank digital currency (CBDC). While different models of CBDC have been proposed, their implementation hinders the current banking system. In this paper, the authors propose a CBDC model, which can be implemented without affecting the current banking system.

I . INTRODUCTION

The emergence of Bitcoin [1] in 2009 inspired by the financial crisis of 2008 has brought upon significant changes in the financial system and the global economy. Bitcoin, an electronic peer-to-peer payment system, allows payments to be made without the need for a financial intermediary. Henceforth, many alternative coins [2] and blockchain [3] platforms have been proposed and developed to provide novel services in the financial area. Due to the services being offered by these blockchain based financial platforms, there is a growing concern of loss in business or fear of being replaced among existing banks and other financial institutions.

Peeking into the banking business, the cost of production and distribution of fiat cash is expensive. The Bank of Korea reports that it costs twice as much to produce coins worth 10KRW and every year bills worth 20 million KRW are subject to damage while 60 billion KRW is invested in reissuance costs [4]. Other shortcomings of cash are loss, theft, burdensome to hold and lack of transparency (as used in funding of illegal activities, terrorism and corruption).

Besides the rise of cryptocurrencies and blockchain-based financial platforms, among other reasons that has sparked interest in the development of central banks digital currencies(CBDC), is the movement towards a cashless society. There are a plethora of applications and payment services offered by third-party payment service providers which have made peerto-peer payments possible without the use of cash. Service providers such as AliPay [5], WeChat Pay [6], M-Pesa [7], etc., boast large user-bases and are able to harness users' payment data and spending habits. These insights are useful to authorities like central banks and governments to establish financial regulations and control over monetary markets. As-is, central banks lack the aforementioned level of authority in the current cashless society. In response, central banks across the globe are making efforts towards the development of CBDCs as a means of cashless payments aimed at reducing cost of production and circulation, facilitating governance and control along with ease to users.

Unlike cash, which is a physical form of money, a CBDC is an electronic form of money issued by a central bank. Simply defined, CBDCs are monetary values stored electronically (digitally, or as an electronic token) that represent liability of the central bank and can be used to make payments [8]. While there is pre-existing electronic central bank money in the form of settlement balances and reserves, these are only accessible to commercial banks and financial institutions. These may be argued as a form of CBDC but these are not the only exclusive forms of CBDC. Different forms of CBDC may be distinguished from their design choices- level of anonymity, accessibility to the general public, border constraints, token-based vs account-based, etc. While there are different perspectives on CBDC, the most general definition of CBDC was illustrated via a venn-diagram by Bech and Garratt (Fig. 1) [9].

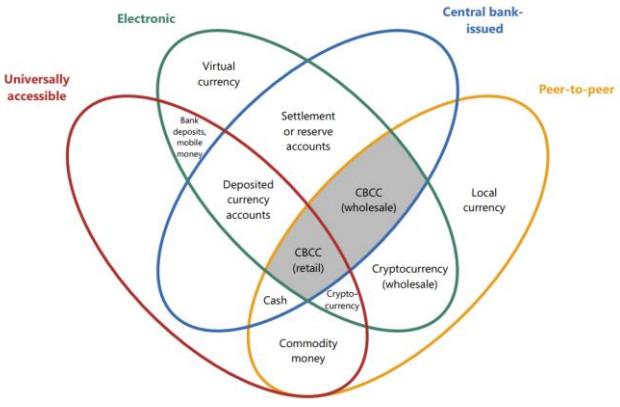

Fig. 1 Money Flower; shaded area represents central bank issued digital currencies.

Based on the above mentioned parameters like accessibility, availability, interest payments, different forms of CBDCs can be defined – Retail CBDC, in which the general public owns a digitized form of central bank money and can be used in retail transactions; wholesale CBDC, in which digital central bank money is issued to banks and financial institutions only for use in large-value transactions; cross-border CBDCs, which facilitates transactions between two countries defined by an exchange rate. Two-tiered CBDCs have also been defined in which commercial banks act as an intermediary to circulate digital currency to the general public. While different forms of CBDCs have been proposed, details on implementation are few.

With the introduction of CBDCs, often discussed is how commercial banks would require to change their business models or even seek other means of making profit. This paper proposes a model of CBDC which is in congruence with the existing banking model. That is, commercial banks can coexist in the CBDC environment without incurring an overhaul of changes. While a small overhead is introduced in the system using the proposed CBDC model, the banking system is benefitted through the added value of blockchain and digital currencies, i.e., less cost of production and circulation, better governance and control. Section II presents related work on CBDC. Section III outlines the design of the proposed model and implementation guidelines. Finally, section IV concludes the paper with potential future work and improvements.

Ⅱ. RELATED WORK

The Bank for International Settlement reports that several nations across the globe have taken an interest in the development, testing, pilot or feasibility analysis of different CBDC projects. Engert and Fung point out the motivation behind CBDCs and their implications on the financial system [8]. The Bank for International Settlements presents a taxonomy on different forms of CBDCs, their design considerations and challenges in their implementation [10]. The International Monetary Fund (IMF) categorizes different forms of money currently in use in the global payment landscape [11]. The IMF argues that e money offered by third party payment service providers are the most widely used forms of payment and that banks must either cooperate or compete with them to dominate the payments market. In the paper, IMF introduces the concept of Synthetic CBDCs whereby central banks and e-money service providers collaborate in a non-zero sum game fashion to increase individual benefits. Additionally, World Economic Forum provides a guideline for policy makers to undertake/deploy a particular form of CBDC given different design requirements [12].

While there are numerous undertakings on surveying the feasibility, application benefits, design considerations and challenges to the development of CBDCs, there are only a handful of papers describing the technical details in implementation. Danezis and Meiklejohn have proposed RSCoin, a cryptocurrency framework in which central banks maintain complete control over the monetary supply, but rely on a distributed set of authorities or mintettes to prevent doublespending [13]. RSCoin builds upon the limitations of Bitcoin – wasteful hashing and lack of governance, and proposes a centralized control of monetary supply henceforth increasing the scalability and stability in the system. Wust et al. have proposed PRCash, a blockchain based currency with central governance which makes use of zero-knowledge proofs and homomorphic encryption to hide the details of transactions [14]. As opposed to RSCoin which focuses on scalability of transaction processing, PRCash focuses on user anonymity while also guaranteeing governance and regulation.

In this paper, we present a CBDC model based on a permissioned blockchain architecture which can be implemented in the current banking environment with only a few changes. The details of the proposed model is discussed in the section below.

Ⅲ. DESIGN & IMPLEMENTATION

A. Requirements

The proposed CBDC model is expected to solve the existing problems of banking environment, i.e., cost of production and circulation of physical cash as well as have features such as better transparency and control. Any digital currency system is able to overcome the inherent problems of fiat cash. Payment service providers like AliPay, WeChat Pay provide direct supply of e-money from supplier to user without intermediaries. However, such payment services could not incorporate the current banking environment where there are intermediaries like commercial banks and financial institutions. The proposed CBDC model must not bring a massive overhaul of the banking system. Commercial banks should not need to seek new avenues of business. Also, the proposed CBDC model should be simple and easy to use (less technically difficult) as people can be reluctant to learn new technology. This can be ensured by user-friendly design of user applications.

We also point out the roles of central banks, commercial banks and users in the system. Central banks will be responsible for the creation of digital currency, enrollment of commercial banks into the CBDC model and distribution of digital currency to commercial banks. Contrary to the existing banking models, central banks will have an added responsibility of registering users under their domain. This is done so as to gain better transparency of users' assets and holdings. Commercial banks will be responsible for enrolling users into their own domain accounts while providing other financial services such as loans, deposits and interest payments. Commercial banks will also need to map users based on their accounts with the accounts held at central banks. General users will be required to enroll under central

bank accounts before registering under commercial bank accounts. General users will also be able to do peer-to-peer transfers via a web or a mobile application without transaction fees.

We also propose a blockchain-based solution compared to centralized database as blockchain based system can providebetter transparency, redundancy and greater system availability. Off-the-shelf enterprise solutions are expensive and not easily customizable. On the other hand, open-source blockchain based payment systems are free to use and can be customized to support financial applications provided by commercial banks (via integration with smart contracts). Central banks will maintain greater control and authority over the blockchain while commercial banks and general users will be appending data to the blockchain when conducting transactions.

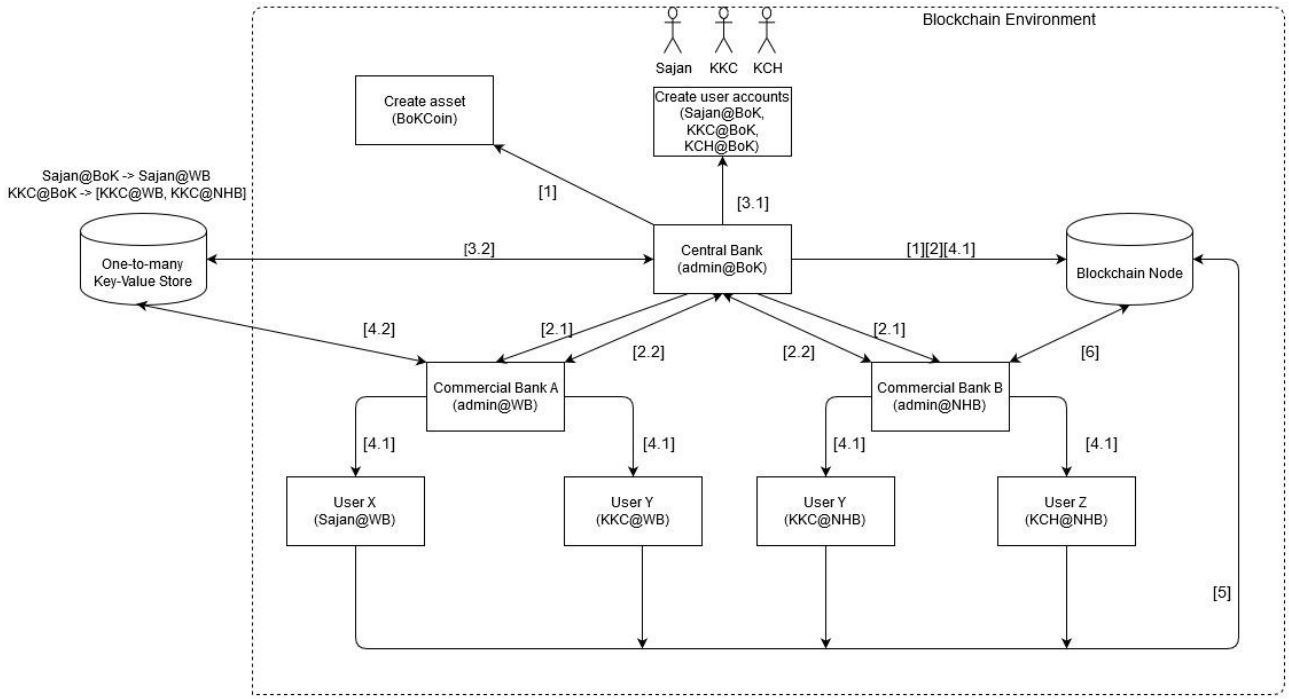

Fig. 2 Proposed CBDC system architecture

B. Design

The overall CBDC architecture shows how different entities in the system interact with the blockchain (Fig 2).

Under the above proposed architecture, the CBDC model is setup as follows-

1 The central bank creates a digital currency for operation in the blockchain platform. Currency issuance is recorded in the blockchain.

2.1 The central bank registers various commercial banks into the blockchain platform. Accounts of commercial banks are written to blockchain.

2.2 The central bank circulates the newly created digital currency to commercial banks. Bidirectional arrow here indicates that commercial banks may pay back the circulated coins at a later time. These transactions are also appended to the blockchain.

3.1 Users interested to participate in the system are only approved after creating accounts with the central bank.

3.2 The central bank records the user details into a key-value store. The key is the account id created at the central bank while the value contains the list of accounts that would be created at other commercial banks. This step enables tracking assets/currency of a user distributed among different banks.

4.1 Users interested in services offered by commercial banks register under accounts of corresponding banks.

4.2 Commercial banks update the key-value store maintained by central banks.

5 Users conduct transactions between themselves (peer-to-peer transfer) and transaction data is recorded in the blockchain.

6 Commercial banks at a later time can conduct different transactions (for example, on behalf of clients, offering of additional services, etc). These transactions are also appended to the blockchain.

The above system architecture depicts the operation under a single node. Multiple nodes can be set up when there are a diverse set of users distributed geographically. In such a scenario, a user can access the nearest node and send transactions via a user interface, for example a web application. The blockchain platform should provide Application Programming Interfaces (APIs) that can be used to interact with the blockchain through the web application (Fig. 3).

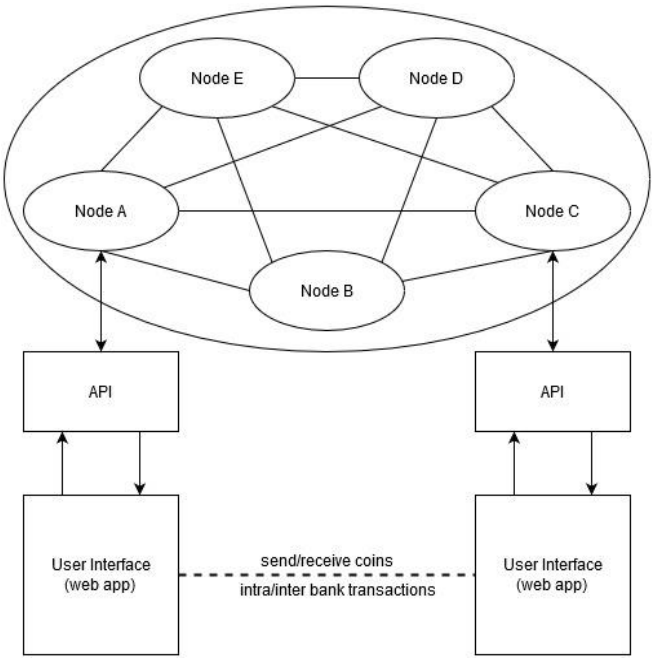

Fig. 3 User interaction mechanism with the blockchain platform in CBDC setting

Traditionally, commercial banks are also responsible for providing additional financial services like loans and deposits, installments, interest payment and other schemes to the general public beside the perfunctory role of currency circulation. The proposed CBDC model considers these services offered by commercial banks through the means of smart contracts [15]. Smart contracts allow automated execution of transactions when certain conditions are met. Financial services such as interest accrued on deposits and loans, tax calculations, installment payments can be smoothly executed via smart contracts. In our model, commercial banks offer these services by deploying smart contracts on top of the blockchain platform (Fig. 4).

Thus, we argue that the proposed CBDC model fits better with the current banking environment than other models of CBDCs that have been suggested. These suggested models argue that the CBDC approach could affect banking business whereby commercial banks are obliged to change their business model and seek other ways of making profit. By using the proposed models, governance and control can be maintained by central banks while still facilitating the commercial banks business models.

C. Implementation Guideline

The development of the proposed model is currently a work-in-progress. The authors suggest that such development be made by using the Hyperledger (HL) [16] blockchain environment. Specifically, under the Hyperledger foundation, the HL Iroha [17] project offers a permissioned blockchain system that can be used to manage digital assets and are used in applications related to interbank settlements, CBDCs, payments systems, etc. The HL Iroha platform can also be integrated with another project under the HL foundation, HL Burrow [18], which allows easy integration of smart contracts on top of HL Iroha. To build the front-end for users, HL iroha offers various software development kits (SDKs) for web and mobile applications for example, Python and Android.

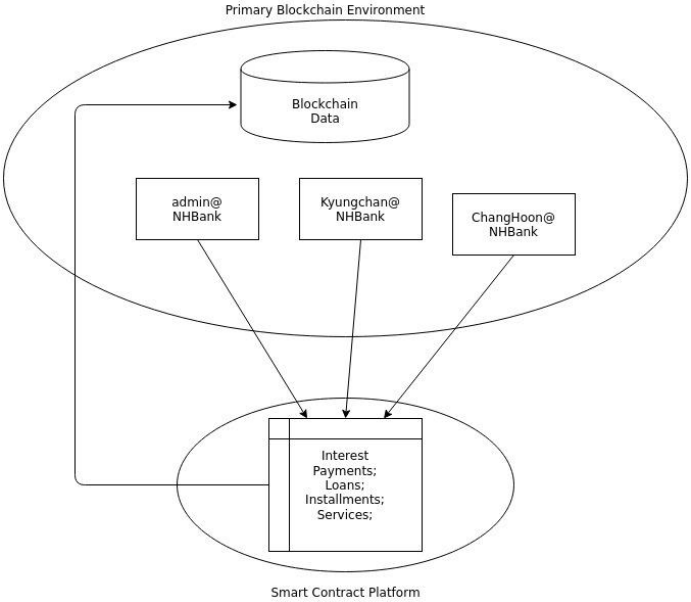

Fig. 4 Services offered by commercial banks are executed by the means of smart contracts

Ⅳ. CONCLUSION

The concept of CBDCs is on the rise in recent years, garnering attention from several governments and central banks. While different models for CBDCs are being proposed and suggested, their implementation is being hindered due to its impact on the current banking systems. In this paper, the authors have suggested an applicable model for CBDC which can be implemented without requiring an overhaul of the current banking system. Central banks will issue coins and govern transactions within the system, while commercial banks will circulate the currency and provide additional services to individuals by the means of smart contracts. Overall, the suggested model of CBDC benefits from the added value of CBDCs (cost of production and distribution, control, transparency) without impacting the current banking system.

The proposed system is currently under development which uses python-sdk for providing user interface through a web application and operating under a single node. When the system needs to be scaled with respect to the high demand from users, web applications could be replaced by providing user interface through mobile applications (android-sdk) and deploying multiple nodes. The authors have only proposed a prototype for the proposed model and thorough testing of system scalability will be done in the near future.

ACKNOWLEDGMENT

This work was supported by the ICT R&D program of MSIT/IITP. [No.2018-0-00539, Development of Blockchain Transaction Monitoring and Analysis Technology]

REFERENCES

[1] S. Nakamoto. "Bitcoin: A peer-to-peer electronic cash system", 2008. (https://bitcoin.org/bitcoin.pdf)

[2] Yuval Gov, "Altcoins - The complete guide". CryptoPotato. (https://cryptopotato.com/altcoins-the-complete-guide/)

[3] Crosby M, Pattanayak P, Verma S, Kalyanaraman V. "Blockchain technology: beyond bitcoin" in Applied Innovation Review Issue 2, June 2016. (https://j2-capital.com/wpcontent/uploads/2017/11/AIR-2016-Blockchain.pdf)

[4] Jin-Bae Kim. "[What is Block] Central Bank issues digital currency, 'CBDC' ". BlockMedia. (https://www.blockmedia.co.kr/archives/114942)

[5] AliPay Inc. "AliPay". (https://intl.alipay.com/)

[6] Tencent. "WeChat Pay". (https://pay.weixin.qq.com/index.php/public/wechatpay_en)

[7] Hughes N. & Lonie S. "M-PESA: Mobile money for the 'unbanked': Turning cellphones into 24-hour tellers in Kenya" in Innovations: Technology, Governance Globalization Issue 2, 2007. (https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/innovationsarticleonmpesa_0_d_14.pdf)

[8] Walter, E. and Fung, Ben S.C. "Central Bank Digital Currency: Motivations and Implications", Bank of Canada Staff Discussion Paper, 2017. (https://www.bankofcanada.ca/wp-content/uploads/2017/11/sdp2017-16.pdf)

[9] Bech, M and R Garratt. "Central bank cryptocurrencies" in BIS Quarterly Review, Bank for International Settlements, September 2017. (https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf)

[10] Committee on Payments and Market Infrastructure. "Central Bank Digital Currencies", Bank for International Settlements, March 2018. (https://www.bis.org/cpmi/publ/d174.pdf)

[11] Adrian, T. & Mancini-Griffoli, T. "The Rise of Digital Money. Fintech Notes", International Monetary Fund. 2019. (https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097)

[12] Center for the Fourth Industrial Revolution. "Central Bank Digital Currency Policy-Maker Toolkit", World Economic Forum. 2020. (http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf)

[13] George Danezis and Sarah Meiklejohn. 2016. "Centrally Banked Cryptocurrencies" in 23nd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016. (https://arxiv.org/pdf/1505.06895.pdf)

[14] Karl Wust, Kari Kostiainen, Vedran Capkun, and Srdjan Capkun. "PRCash: Fast, Private and Regulated Transactions for Digital Currencies." In Financial Cryptography and Data Security - 23rd International Conference, FC 2019. (https://doi.org/10.1007/978-3-030-32101-7_11)

[15] Nick Szabo. "Smart Contracts: Building blocks for digital markets". 1996. (http://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf)

[16] The Hyperledger Foundation, "Hyperledger". (https://www.hyperledger.org/)

[17] The Hyperedger Foundation, "Hyperledger Iroha". (https://www.hyperledger.org/projects/iroha)

[18] The Hyperledger Foundation, "Hyperledger Burrow". (https://www.hyperledger.org/projects/hyperledger-burrow)