A Blockchain-based Framework for Central Bank Digital Currency

Xuan Han[1,2], Yong Yuan[1,2], Fei-Yue Wang[1,2,3]

1. The State Key Laboratory for Management and Control of Complex Systems
Institute of Automation, Chinese Academy of Sciences, Beijing, China
2. Qingdao Academy of Intelligent Industries, Qingdao, China
3. Research Center of Military Computational Experiments and Parallel System,
National University of Defense Technology, Changsha, China
Email: xuan.han@ia.ac.cn, yong.yuan@ia.ac.cn, feiyue.wang@ia.ac.cn

Abstract—**Cryptocurrency and blockchain technologies have developed in parallel in recent years, with technological breakthroughs in currency issuance, payment methods, and currency storage. However, the existing cryptocurrencies cannot replace fiat money. There is a huge gap between decentralized cryptocurrency and central bank digital currency, namely CBDC, in terms of monetary governance and circulation. In this paper, we propose the function and security requirements of CBDC, through a comprehensive analysis of the existing typical cryptocurrency and the prototype of the CBDC scheme. On this basis, we present a blockchain-based framework for CBDC with three layers, including supervisory layer, network layer and user layer, and describe the key business processes of the CBDC's entire lifecycle of issuance-circulation-withdrawal in detail. Finally, we take cross-border payment as an example to explain the transaction process of CBDC. We aim to provide theoretical guidance for CBDC design.**

Index Terms—**Central bank digital currency, blockchain, cryptocurrency, currency issurance, currency circulation**

I. INTRODUCTION

Cryptocurrencies originated from blind signature technology, aimming to solve the problem of anonymous payment [1]. The original E-Cash was a centralized, untraceable electronic payment scheme relying on central banks to process and validate transactions [2]. The emergence of Bitcoin and blockchain technology has overcome the long-term dependence of electronic payment on trusted third parties [3]. Subsequently, cryptocurrencies based on blockchain are gradually becoming decentralized.

After more than 10 years of development, hundreds of cryptocurrencies based on blockchain have emerged, creating a series of influential innovations in all aspects of financial markets and the wider economy [4], [5]. In particular, the potential impact of cryptocurrencies and blockchains on retail payment services is crucial. These schemes make peer-to-peer payments easier and cheaper, and have the potential to facilitate e-commerce, cross-border transactions and some retail payment transactions [6], [7].

Cryptocurrencies such as Bitcoin based on blockchain have some monetary characteristics, however, there are still significant differences between the decentralized cryptocurrencies and fiat money [8]. First, these cryptocurrencies are neither issued by any sovereign institutions, nor recognized by governments or trusted entities. In addition, decentralized cryptocurrencies are designed and maintained by various untrusted third-party agencies to actively develop and operate cryptocurrency and distributed blockchains, which may raise regulatory issues for central banks or other regulatories. If decentralized cryptocurrencies are widely circulated, their impact on payment system supervision, regulation, financial stability and monetary policy may become more prominent.

The concept of central bank digital currency, CBDC, was proposed in order to comply with the digital development trend. CBDC can control the chaos of cryptocurrency schemes, stabilize the financial payment markets and bring new opportunities for traditional financial infrastructure. It is not only the digital expression of fiat money, but a sovereign currency recognized by the state sovereignty, issued by the central bank and denominated in a specific fiat currency. It is usually issued, traded, retrieved and stored through encryption algorithm and other digital technologies.

At present, many countries take a positive attitude towards the research and development of CBDC, believing that it can reduce issuing cost and increase transaction convenience. Among them, the Bank of England commissioned of University of London to develop a CBDC scheme, namely RSCoin, which was the first CBDC system proposed by the central bank [9]. The Bank of Canada has been carrying out an experimental project called "Jasper", which aims to explore and create a payment system with CBDC technology, and will eventually launch the digital Canadian dollar, called CADCoin [10]. China has established the digital currency research institute in 2014, and has taken the lead in formulating the strategic goal of developing CBDC, planning to release the CBDC system in 2019.

Although the cryptocurrencies have made some progress, they cannot be directly used in CBDC design, due to the difference between CBDC and cryptocurrencies. Meanwhile, there are fewer CBDC programs published, which adds some difficulties to CBDC research and development. From the technical perspective, CBDC are facing the following challenges.

1. What functions and security properties does CBDC need

to implement?

2. How to construct a CBDC framework to realize the function of physical currency?

For the first question, CBDC should not only meet the functionalities of fiat money in the circulation process, including the value scales, circulation means, value storage and payment means, but also should overcome new security challenges in the process of fiat money. As far as the framework design of legal digital currency is concerned, there are two mainstream models, account-based and wallet based. Account-based model can be built on the existing banking system and can achieve a high degree of integration between CBDC and the existing banking system. Wallet-based model is widely used in cryptocurrencies, which is more conducive to anonymous payment.

Blockchain plays an important role in the research and development of cryptocurrency, which can also be conducive to the establishment of secure payment and trust system of CBDC. Blockchain is an innovative technology with extensive application potential, which can not only be used as the network structure of payment system, but also may be adopted by financial market infrastructure (FMI), having a positive impact on the financial system and other networks in the whole economy [6], [7].

In this paper, we take efforts to propose a CBDC framework based on blockchain. First, we study the existing cryptocurrencies and CBDC samples, and induce the functional characteristics and security properties that CBDC should to meet. Then, we present a three-layer structure of CBDC framework based on blockchain, including regulatory layer, network layer and user layer, and introduce the key business processes in the life cycle of CBDC in detail, such as identity authentication, currency issuance, circulation and withdrawal. Finally, we take cross-border payment as a use case to explain CBDC's business process and the feasibility of CBDC's three-layer framework.

The remaining part of the paper is organized as follows. In Section II we introduce the backgrounds of cryptocurrency and CBDC, and analyze the differences between them. In Section III, we induce the functional characteristics and security properties that CBDC should to meet. In Section IV, we propose a three-layer structure of CBDC framework based on blockchain, including regulatory layer, network layer and user layer. In Section V, we introduce the key business processes in the life cycle of CBDC in detail. In Section VI, we explain how CBDC works to achieve cross-border payment. Finally, we conclude our construction briefly in Section VII.

II. BACKGROUND

A. Cryptocurrency

With Bitcoin as the boundary, cryptocurrencies can be divided into two stages: the cryptocurrencies represented by E-Cash and the decentralized cryptocurrencies based on blockchain. It should be noted that electronic currency, virtual currency and digital currency are collectively referred to as cryptocurrency in this paper, although they are slightly different in design and application.

In 1983, Chaum constructed the first cryptocurrency scheme using blind signature [1]. He constructed an anonymous electronic payment scheme based on RSA-based blind signature algorithm in 1985, which has auditability, controllability and anonymity to some extent [2]. It was a classic case of centralized crytocurrency with a three-party model of bank-user-merchant, which laid a foundation for centralized cryptocurrencies. In order to improve payment efficiency, Camenisch et al constructed a compressed crytocurrency scheme, E-Cash, under the assumption of RSA and DDH [11]. The following research considered the splitting and fusion of currencies on the basis of E-Cash, so as to enhance the usability. Although the centralized cryptocurrency schemes initially realized security, anonymity and traceability, there were serious efficiency problems left and didn't consider complex payment scenarios.

Bitcoin was born in 2008, which alleviated the efficiency problem of centralized cryptocurrencies [3]. The use of hash function, blockchain structure and digital pseudonym partly ensured the security and anonymity of payment process. Subsequent research focused on the security, anonymity and efficiency of decentralized cryptocurrency. In 2015, Garay et al abstracted the backbone protocol of Bitcoin in the static synchronous network model and provided the security definition and proof framework of Bitcoin [12]. Monroe and Zerocash successively used ring signature and zero-knowledge proof to enhance the anonymity of payment. In response to the efficiency of Bitcoin, a series of new consensus protocols and payment methods such as PoS Protocol, sharding protocol, and lightning network were proposed.

B. Central Bank Digital Currency

CBDC is generally defined as the value of digital representation, electronic storage, and cryptographic transfer, that is expressed digitally, stored electronically, and encrypted for transfer of ownership. It is issued and managed by a sovereign institution such as the central bank, subject to the laws and regulations applicable to a specific jurisdiction. CBDC is another form of fiat money, similar to coin and banknote, which can be effectively exchanged for cash in denominations.

RSCoin, proposed by the University of London, is the first CBDC framework published [9]. However, it only gives the grouping architecture based on blockchain, without in-depth discussion on currency issuance, regulation, anonymity and other aspects. At present, there are still many problems in the requirement design and implementation of CBDC throughout its whole life cycle. First, the functional requirements and security objectives of CBDC are not fully explained. Second, the CBDC infrastructure framework is not clear. There are still doubts about whether to adopt the secondary structure of central bank-commercial bank. Finally, the data structure and storage model of CBDC are not uniform. It is still controversial whether to adopt the wallet or account based model. These have hindered the development of CBDC and made it stagnant.

C. Differences between Decentralized Cryptocurrency and CBDC

Some decentralized cryptocurrency schemes can implement anonymous payment, secure storage and so on [13], but there are still significant functional differences between them and CBDC, as shown in the following aspects:

Currency value: The price of decentralized cryptocurrencies is determined by the supply and demand relationship, depending on the belief that they may be exchanged for a certain number of goods or fiat money. Their prices fluctuate so much that they cannot act as general equivalents as fiat money issued by sovereign institutions.

Issuance and supply: Decentralized cryptocurrencies are issued and distributed by pre-agreed computer protocols, without the endorsement of sovereign entities. Different protocols could cause problems such as supply shortages or inflation.

Payment method: Cryptocurrencies based on blockchain appear to enable peer-to-peer payments between users and merchants without the trusted third parties. However, when cryptocurrency is exchanged with other types of currencies, it is necessary to rely on third-party exchanges, which may pose security risks.

Regulatory approach: In decentralized cryptocurrencies, it is difficult to modify and revoke the transactions recorded in the ledgers. This is a security attribute of blockchain, but also creates conditions for illegal transactions to flourish. Due to the lack of regulatory means, these cryptocurrencies are likely to be subjected to money laundering, extortion and other crimes.

D. Blockchain in the Field of Payment

Blockchain is a key innovation in decentralized cryptocurrencies [13], allowing remote peer-to-peer value transfers between parties without a trusted third party. The factors that blockchain may affect the development of payment industry and CBDC include:

Cost: Blockchain-based payment systems may offer lower transaction cost than other payment methods, especially in cross-border payment, currency exchange and other payment scenarios involving multiple intermediary entities.

Usability: Compared with traditional payment methods, blockchain-based payment methods have some usability advantages, because the blockchain makes the transaction process more intuitive and easier to integrate with other services.

Anonymity: Although the blockchain itself does not provide any privacy protection, it provides an effective network architecture for anonymous payment. Some blockchain-based cryptocurrency schemes allow users to conduct transactions without providing their own real credentials.

III. KEY FEATURES OF CBDC

In this section we describe the features of both the currency and security aspects that CBDC needs to meet. The currency functions to be implemented by CBDC include centralized issuance, transferability, storability, offline transaction, exchangeability, and controllable regulation. Considering the digital nature of CBDC, the security properties it seeks include no double-spending, unforgeability, non-repudiation, verifiability and anonymity.

A. Functions of CBDC

Centralized issuance: Centralized issuance is the most obvious feature of CBDC that differs from the general cryptocurrencies. It means that CBDC is backed by the sovereign states or central banks. The monetary policy is formulated by the centralized sovereign institution, so that CBDC has the intrinsic value.

Transferability: It refers that CBDC can be used as a means of circulation and payment for ongoing value movements in economic activities. In the actual payments, CBDC also needs to achieve the split maintaining the zero-sum principle for more efficient and convenient circulation.

Storability: CBDC and the transaction history are securely stored in the form of electronic data in an organization or user's electronic device for query, payment, exchange and management.

Offline transaction: It is impossible to achieve complete offline trading like physical currency in the digital world. Offline transaction of CBDC specifically means that it may not directly communicate with the host servers or the main system when the transaction is performed through the electronic device, and the payer does not exchange information with other devices or systems through communication methods such as wired or wireless.

Exchangeability: In the circulation of CBDC in the digital world, it is also necessary to satisfy the exchangeability, including the equivalent exchange between one CBDC and other forms of the same sovereign currency, as well as the foreign exchange between CBDC and other sovereign currency CBDC.

Controllable regulationIn order to prevent the use of CBDC for the implementation of illegal economic activities, CBDC also needs to achieve controllable regulation both in terms of policy and technology. Although regulation has sacrificed decentralization and anonymity to some extent, it is an important means of creating a good legal digital currency financial environment.

B. Security Properties of CBDC

- No double-spending: No double-spending means that once a CBDC owned by a user has been transferred, it cannot be used to pay for other transactions. Unlike a physical currency, CBDC, uniquely identified by a sequence of serial numbers, can be copied and saved multiple times. Therefore, no double-spending is the basic security that all digital currencies need to consider.

- Unforgeability: Unforgeability requires that no one can falsify CBDCs issued by the sovereign institutions or forge a CBDC that is not owned by him/her. These forged CBDCs cannot pass verification. CBDC also requires anti-counterfeiting technology to ensure currency security, just like physical currency.

- **Non-repudiation:** Non-repudiation requires that all participants' actions be recorded from the initiation of the transaction to the end, including the payer, the recipient, and the transaction verifier. No one can deny the transaction steps that he has completed.
- **VerifiabilityVerifiability** requires that all transaction records involved in the CBDC system can be validated effectively. This is crucial for CBDC as a currency of circulation and a means of payment. It is also the basis for other security properties.
- **Anonymity:** The physical currency is anonymous in actual circulation. Similarly, CBDC should also be designed for user privacy and anonymity. Throughout the development of cryptocurrencies, the anonymity of CBDC mainly includes anonymity of identity and anonymity of transaction. Intuitively, they require that any unauthorized user cannot obtain, calculate, or infer the identity of a user and the information of a transaction through open source data.

IV. A BLOCKCHAIN-BASED FRAMEWORK FOR CBDC

In this section, we present a three-layered CBDC framework based on blockchain, followed by the regulatory layer, network layer and user layer. It should be noted that in this section, we have a rare discussion of the specific blockchain design and other technical details. We assume that enabling capabilities are available to be incorporated with blockchain, and that the blockchain schemes implemented will be secure and scalable to design targets.

A. Regulatory Layer

Regulatory layer is the main difference between a CBDC scheme with centralized issuance and the decentralized cryptocurrency architecture. Regulatory layer is mainly in charge for controlling and governing the whole life cycle of CBDC throughout the technical and policy aspects, so as to maintain the healthy and stability of the financial environment dominated by CBDC. Regulatory layer mainly includes central bank, public key infrastructure (PKI) with identity authentication as the core, and other regulatory bodies such as sovereign institutions. They aim to implement the supervision of objects such as banks and third parties in network layer and users and transaction in user layer. Regulatory layer are not completely centralized. Regulatory bodies need to cooperate and restrict each other.

B. Network Layer

Network layer is a bridge between the top regulators and ordinary users. It is different from the p2p network structure mostly adopted by decentralized cryptocurrencies, network layer in CBDC adopts two different network structures. One is a tree hierarchy structure centered on central bank and other regulatory agencies, and the other is a local distributed structure composed of commercial banks and other third-party operators. The centralized tree hierarchy could help CBDC better integrate with the existing bank financial structures and facilitate the implementation of regulation. The local distributed structure can utilize blockchain to solve the centralized load problem, enrich the financial organization structure, and provide users with convenient, fast and diverse ways of payments. It can also increase business interactions between banks and other third-party operators, and enhance the security and trustworthy of CBDC network layer.

C. User Layer

User layer consists of the low-level users and their transactions, which are not only the regulatory objects of regulatory layer, but also the main data source for verification and processing of network layer. user layer includes cash exchange, CBDC deposit, CBDC withdrawal, inter-bank payment, cross-bank payment, cross-border payment and currency exchange. When the users of user layer submit transactions, they treat the network layer structure, transaction processing and regulatory operations of the upper layers as black boxes.

V. BUSINESS PROCESS FLOW OF CBDC

In this section, we give the business process flow of CBDC throughout the whole lifecycle of issuance, circulation and withdrawal.

Fig.1 shows the three-layer structure of CBDC, and illustrates the main business processes such as identity management, currency issuance, circulation and repatriation in detail.

A. Identity Authentication

Identity authentication is an important means to ensure operators have legal digital identity, and it is the basis of establishing CBDC system framework. Authentication in CBDC includes the generation of users' identity, the certificate authority (CA) of commercial banks and third-party operators. The specific business process is as follows:

1. CA issues CA certificates to commercial banks and third party operators authorized by the central bank to grant them legal digital identities.
2. Branches in commercial banks that adopt a tree-level hierarchy may be sub-branched by their head offices. The IDs of the branches have the attributes of their head offices.
3. Users can apply for different identities and account addresses through different commercial banks, which have corresponding identity attributes of the opening bank.
4. Users can also apply for a legitimate digital identity and account address from a third-party operator that has obtained a CA certificate. The different IDs of one user are associated with the user's unique physical identity.
5. Central bank can query and verify the identity information of a certain institution and user from CA.

B. Currency Issuance

CBDC issuance is functionally similar to coinbase transactions in Bitcoin or mint transactions in Zeracash, except that CBDC is issued by a central bank or a regulatory agency authorized by a sovereign authority which follows a
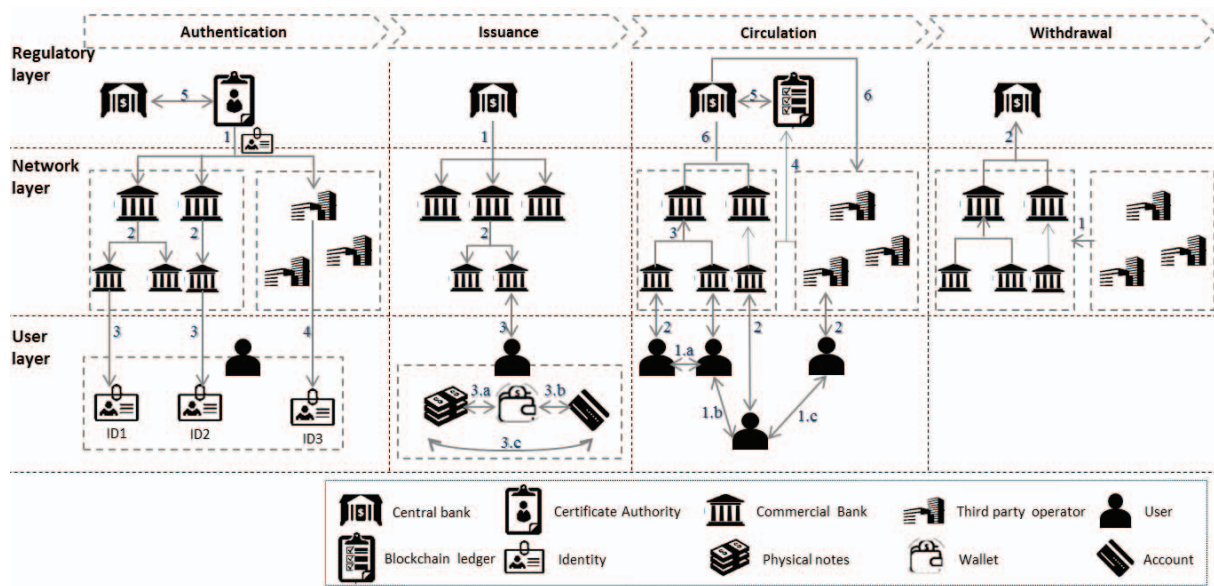
266

Fig. 1. The three-layer architecture and business processes in CBDC

reasonable and legal monetary policy, while currency issuance in cryptocurrency relies on the protocols agreed in advance. CBDC issuance adopts a tree hierarchy structure with a central bank as the root node, and finally reaches the circulation among users through commercial banks. The specific business process is as follows.

1. Central bank allocates CBDC to various authorized commercial banks after signature by mint transaction or other means.
2. The commercial banks will assign the CBDC they received to their branches.
3. Finally, users obtain CBDC through currency exchange, withdrawal, and other means.

CBDC can be stored and used in both wallet-based and account-based forms, for the convenience of currency circulation and storage. A user can exchange physical fiat money with wallet-based CBDC, transfer of CBDC between his wallet and his account, and exchange physical fiat money with account-based CBDC within the same ID.

C. Currency Circulation

The circulation of CBDC mainly describes the whole business process from the user submitting the CBDC transaction to the transaction being finally recorded into blockchain ledger, which is the core functionality of CBDC. The specific business process is as follows:

1. A user selects an ID that he/she owns and creates a transaction on a client provided by a commercial bank or a third party operator that corresponds to the ID. The transactions users can create include: a. inter-bank payment, b. cross-bank payment, c. cross-border transfer, etc.
2. The user submits a transaction to the corresponding commercial bank branch or third-party operator. Com-

mercial banks and third-party operators are in charge for transaction verification, recording and management of account and wallet during CBDC circulation. Commercial banks and third-party operators also report back to the user the results of the transaction execution.
3. After receiving the transaction submitted by the user, the commercial bank branch verifies it and executes the anti-money laundering (AML) operations, and then submits the transaction and verification result to the upper commercial banks.
4. Commercial banks and third-party operators submit the verified transactions to the blockchain network, and record them in the blockchain ledger through a consensus protocol.
5. Central bank can access the blockchain ledger and monitor users' transactions.
6. Central bank also supervises all operations of commercial banks and third party operators.

D. Currency Withdrawal

CBDC withdrawal is a function of symmetry with CBDC issuance, reflecting the balance of payments of banks as well as the economic situation. CBDC withdrawal is also beneficial to update CBDC versions, enhance functionality and security. The main process is as follows:

1. The third party operators neither directly participate in CBDC issuance nor directly submit CBDC withdrawal to the central bank, but realize CBDC withdrawal and expenditure through business dealings with the commercial banks.
2. Commercial banks submit CBDC from the underlying branches level by level. Finally, CBDC is reclaimed by central bank in accordance with the monetary policy.

267

VI. Cross-border Payment by CBDC

In order to better introduce the advantages of the CBDC framework, we provide the use case for cross-border payment using CBDC in this section.

Cross-border payment refers to the completion of value transfer across geographical boundaries through multiple fiat currencies. It is an important use case for CBDC design. Conducting cross-border payment through CBDC could provide real-time settlement and reduce costs, enabling new business models, and institute new models of regulatory oversight. We use cross-border payment as a use case to explain the payment process of the CBDC framework, as shown in Fig.2.
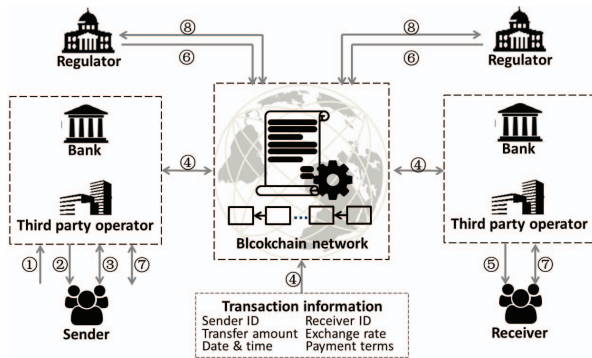

Fig. 2. Cross-border payment process in CBDC

1. The sender creates a transaction under an ID he owns and submits it to the corresponding bank or third party operator.
2. Upon receiving a transaction request, the bank or third party operator performs AML operations to verify whether the transaction is in compliance.
3. If the transaction is compliant, the bank or third-party operator locks the CBDC within the transaction. If not, the bank or third party operator will report the transaction failure message to Sender.
4. The bank or third party operator of the sender interacts with the bank or third party operator of the receiver through blockchain network, using the transaction information as a trigger to start the cross-border payment smart contract. And then the cross-border payment smart contract begins to execute.
5. The bank or third party operator of the receiver performs AML operations to verify that the receiver and the transaction are in violation.
6. The bank or third party operator of the receiver performs AML operations to verify that the receiver and the transaction are in violation.
7. If the cross-border payment smart contract is successfully executed, the bank or third party operator of the sender feeds back the transaction success message to the sender and updates the sender's CBDC account or wallet information; the bank or third party operator of the receiver sends a receipt message to the receiver. Meanwhile, the receiver can unlock the CBDC and keep it in his wallet

or account. If the execution fails, the bank or third party operator of the send feeds back the transaction failure message to the sender and unlocks the CBDC.
8. The regulators may also query, verify and recover the transaction after the transaction is over.

VII. Conclusion

In this paper, we analyzed the functional differences between decentralized digital currency and CBDC in detail, and then give the security and functional requirements that CBDC should meet. On this basis, we further proposed a blockchain-based framework for CBDC with three layers, including the supervision layer, network layer and user layer. In addition, we introduced the key business processes of CBDC. Finally, we introduce the transaction processing flow of CBDC by taking cross-border payment as an example.

References

[1] D. Chaum, Blind signatures for untraceable payments, *in Annual International Cryptology Conference(CRYPTO 1983)*, Boston, MA, 1983, pp.199-203.
[2] D. Chaum, Security without identification: Transaction systems to make big brother obsolete, *Communications of the ACM*, 1985, Vol. 28, No. 10, pp.1030-1044.
[3] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Accessed: Feb. 23, 2019, [online]. Available: http://bitcoin.org/bitcoin.pdf, 2008.
[4] R. Qin, Y. Yuan, F. Wang, Research on the selection strategies of blockchain mining pools, *IEEE Transactions on Computational Social Systems*, 2018, Vol. 5, No. 3, pp.748-757.
[5] J. Zhang, F. Wang, X. Wang, *et al*., Cyber-physical-social systems: The state of the art and perspectives, *IEEE Transactions on Computational Social Systems*, 2018, Vol. 5, No. 3, pp. 829-840.
[6] F. Wang, Y. Yuan, C. Rong, *et al*., Parallel blockchain: An architecture for CPSS-based smart societies, *IEEE Transactions on Computational Social Systems*, 2018, Vol. 5, No. 2, pp. 303-310.
[7] F. Wang, Y. Yuan, J. Zhang, *et al*., Blockchainized internet of minds: A new opportunity for cyber-physical-social systems, *IEEE Transactions on Computational Social Systems*, 2018, Vol. 5, No. 4, pp. 897-906.
[8] B. Qin, L. Chen, Q. H. WU, *et al*., Bitcoin and digital fiat currency, *Journal of Cryptologic Research*, 2017, Vol. 4, No. 2, pp.176-186.
[9] G. Danezis, S. Meiklejohn. Centrally banked cryptocurrencies Accessed: Mar. 19, 2019. [Online]. Available: https://arxiv.org/abs/1505.06895, 2015.
[10] R. Garratt. CAD-coin versus Fedcoin Accessed: Mar. 24, 2019. [Online]. Available: https://www.r3cev.com/s/Cad-coin-versus-Fedcoin-rg.pdf, 2016.
[11] J. Camenisch, H. Susan, L. Anna, Compact e-cash, *in Annual International Conference on the Theory and Applications of Cryptographic Techniques(EUROCRYPT 2005)*, Aarhus, Denmark, 2005, pp.302-321.
[12] J. Garay, A. Kiayias, N. Leonardos, The bitcoin backbone protocol: Analysis and applications, *in Annual International Conference on the Theory and Applications of Cryptographic Techniques(EUROCRYPT 2015)*, Sofia, Bulgaria, 2015, pp.281-310.
[13] S. Wang, J. Wang, X. Wang, *et al*., Blockchain-powered parallel healthcare systems based on the ACP approach, *IEEE Transactions on Computational Social Systems*, 2018, Vol. 5, No. 4, pp. 942-950.