# New application of blockchain: digital currency model design in the context of Winter Olympics

*Zihuan* Feng[1], and *Xun* Liang[1,*]

[1]School of Information, Renmin University of China, Beijing, 100872, China

**Abstract.** With the further expansion of blockchain application ecology, various applications and infrastructure around digital currency are constantly enriched and improved, and the whole market is booming along the healthy track. The Chinese government also attaches great importance to the development and application of block chain technology. President Xi Jinping stressed the importance of the block chain as an important breakthrough in the core technology independent innovation in the eighteenth collective learning of the Central Political Bureau. In October 2020, the pilot project of digital RMB will be launched in Shenzhen. Under the blockchain empowerment, the design, issuance and landing preparation of China's digital RMB have been in the forefront of the central bank's digital currency. Although the technical feature of blockchain is decentralization, the central bank can effectively integrate the distributed operation by using blockchain, so as to better realize the centralized management and control of digital currency. Taking the Beijing Olympic Games as an example, this paper analyzes the problems that may occur in the use of digital RMB in the Winter Olympics, puts forward an assumption of using digital currency based on partial decentralization, and puts forward the overall architecture design, and analyzes its feasibility and practicability.

## 1 Introduction

In May 2020, Gang Yi, governor of the people's Bank of China, said that digital RMB(DC/EP, Digital Currency /Electronic Payment) would be tested in Shenzhen, Suzhou and the future Winter Olympic Games. In October 2020, Shenzhen launched a digital RMB test activity; in December 2020, Suzhou issued RMB 20 million consumption red packets for digital RMB testing. Although digital RMB is not based on blockchain, it still retains the basic characteristics of cryptocurrency, such as anonymity, security, unforgeability and anti double flower, through specific issuance management mode and relevant technical principles, on the basis of ensuring centralized management requirements. Under the blockchain enabling, the design, issuance and landing preparation of China's digital RMB have been in the forefront of the central bank's digital currency [1].

Blockchain technology was born in bitcoin digital currency in 2008. It provides a decentralized credit establishment paradigm without trust accumulation. It is a distributed

* Corresponding author: xliang@ruc.edu.cn

database technology. By maintaining the chain structure of data blocks, it can maintain the continuous growth and unforgeable data records [2]. Blockchain has broad application prospects in the financial field. Major financial institutions all over the world actively participate in the investment of blockchain projects and strengthen the research on blockchain technology, including Nasdaq, Goldman Sachs, Citigroup, Morgan Stanley, UBS, etc. The infrastructure of banks and other financial institutions, combined with the underlying blockchain technology, will have a profound impact on the existing payment, transaction and settlement methods, and improve the efficiency of their operation. Blockchain technology has a wide range of application prospects in finance, credit reporting, Internet of things, asset management and many other fields. With the maturity of blockchain technology, the further expansion of blockchain application ecology, the further development of the number of product users and application scenarios, a variety of digital currency applications and infrastructure are constantly enriched and improved, and the whole market is booming along the healthy track. As a disruptive technology, blockchain is leading a new round of technological change and industrial innovation globally [3]. The Chinese government also attaches great importance to the development and application of block chain technology. General Secretary Xi Jinping stressed the importance of the block chain as an important breakthrough in the core technology independent innovation in the eighteenth collective learning of the Central Political Bureau[4].

Digital RMB can retain the centralized characteristics of traditional legal currency and fit the excellent characteristics of decentralized digital currency, which is exactly the reference of blockchain technology and its concept. However, the decentralized nature of blockchain conflicts with the centralized management requirements of the central bank, The special nature of the central bank requires that its nodes should have the highest authority and regulatory ability. Although the digital currency of the central bank is also combined with the blockchain technology, it is still completely dominated by the state and has sovereign credit. Its essence is centralized, which is contradictory to the characteristics of decentralized blockchain technology [5]. Therefore, digital RMB is still a centralized system. However, the traceability and unforgeability of the data on the blockchain are just what the RMB regulatory field lacks. Based on the blockchain structure, it can largely avoid the occurrence of financial money laundering and make every transaction open and transparent.

Based on the characteristics of blockchain and the functional structure of digital RMB, this paper analyzes the problems that may occur in the use of digital RMB in the relatively closed Winter Olympic Games, taking Beijing stadium of the Winter Olympic Games as an example, puts forward an assumption of issuing and using digital currency based on partial decentralization under the closed scenario, and puts forward the overall framework Design and analyze its feasibility and practicability.

## 2 Application of blockchain in digital currency

Bitcoin is the first application of blockchain, and the most famous implementation is "bitcoin". Bitcoin is a peer-to-peer digital currency, which provides the world with an alternative to the traditional banking system.

Since its appearance in 2009, bitcoin has successfully processed millions of transactions. What's more, bitcoin network has never experienced a large-scale system failure. At present, there are thousands of nodes in bitcoin network, and its P2P network architecture ensures the steady increase of bitcoin transaction volume. From the history of digital currency, bitcoin can be said to be a significant social experiment in the history of finance. It is the first time to realize a real secure and reliable distributed storage digital currency mechanism. Compared with the traditional monetary system, bitcoin solves the problem that the

traditional monetary system is in the hands of individual institutions, and also lays the foundation for the emergence of anonymous transactions [2].

Ethereum is an open-source public blockchain platform with smart contract function. On this platform, users can create new blockchain assets, build new smart contracts, and process point-to-point contracts through virtual machines that provide distributed storage through its dedicated cryptocurrency Ethereum. To create more commercial and non-commercial applications. In this period, the development of blockchain is no longer limited to digital currency, but has been widely used in the financial field. In financial scenarios such as stocks, bonds, futures, crowdfunding, funds and other financial scenarios, blockchain and smart contracts have been involved.

Libra is proposed by Facebook and managed by the Libra association composed of several companies and institutions. Each institution adopts the licensing system to obtain access permission. It is a hybrid architecture combined with blockchain: blockchain is used for top-level clearing and settlement, and centralized processing is used for bottom transactions. Libra is not issued by the Federal Reserve, nor has it been approved by US regulators for the time being [6].

**Table 1.** Comparison of mainstream digital currencies.

| | **Bitcoin** | **Ethereum** | **Libra** | **digital RMB** |
|---|---|---|---|---|
| Users | Coin holders, miners, developers | Institutions of secondary development, holders, miners and developers | All people | All people |
| Smart contract | No | Yes | Yes | No |
| Monetary value | Not equal to legal tender | Not equal to legal tender | Not equal to legal tender | Equal to legal tender |
| Credit guarantee | No | No | No | Yes |
| Consensus process | All nodes | All nodes | A few nodes | A few nodes |
| Type | Public chain | Public chain | Alliance chain | / |
| main features | Blockchain 1.0 The code is clear and simple, and more decentralized | Blockchain 2.0 It is the first large-scale application platform of smart contract | Money without borders + financial infrastructure for billions of people around the world | Mixed structure, no preset route, credit guarantee by the central bank, with legal compensation |

Although the digital RMB does not use the blockchain technology at present, the design of the digital RMB adopts some characteristics of the blockchain and combines the blockchain technology, and it does not exclude the use of blockchain in some scenarios in the future.

# 3 Model design

## 3.1 Problem and Solution

The Winter Olympic Games is an international event held by China. Beijing is one of the three competition areas of 2022 Winter Olympic Games, and it is also one of the pilot projects of digital RMB. The composition of the Winter Olympic Games is very complicated. There are athletes, journalists, spectators, judges, etc. These people come from

different countries and use different currencies. In the process of using digital RMB, there will be various problems. The possible problems and corresponding solutions are listed below.

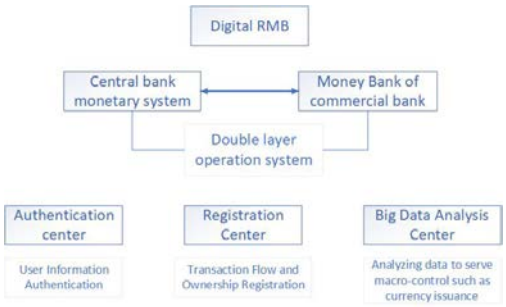


**Fig. 1.** Design Mode of Digital Renminbi "One Currency, Two Treasuries and Three Centers".The "One Money", the central bank's digital currency, is an encrypted string of numbers guaranteed and signed by the People's Bank of China and issued on behalf of a specific amount. " Two Treasuries" refers to the digital currency issuing library and digital currency commercial bank library, which are responsible for the management of currency . The two-tier operation mode is that the people's Bank of China exchanges money with commercial banks, and commercial banks exchange money with people.. The "three centers" include certification centers, registration centers and large data analysis centers.

(1) When the traffic is too large, the network of the central system is congested, and the same digital currency is paid to different people. A partially decentralized blockchain structure can be designed, in which each commercial bank is regarded as a node on the chain, and the bank is responsible for its customers. The bank exchanges information between banks and finally accounts.

(2) During the Winter Olympic Games, the organizers will send a certain number of official tickets to the participants. These official tickets include meal tickets, admission tickets and other forms in previous years, which are paid in advance by using the activity funds. According to the experience of previous years, some staff members or guests will transfer the official coupons to those who are not eligible for the official coupons at will, resulting in great waste. In this case, official coupons can be issued in the form of digital currency, and each official voucher type and amount can be directly recorded in the personal digital currency wallet account and bound with personal identity information. Only digital currency transfer can be turned off. At the end of the event, the remaining digital currency becomes invalid and no longer has payment function, which can save costs. Users can freely pay and transfer their own digital currency.

(3) The audience and guests come from different countries, so the way to obtain digital RMB account needs to be unified. To solve this problem, each user uses his ID card or passport to apply for an account, and each user is given a unique identification code, which can not be changed. The registration information of each user is recorded, and the currency exchange rate is exchanged between the commercial bank and the Central Bank of the user's country. The user can directly use digital RMB for payment.

(4) Every year, we can see the news of fake currency. On such a big occasion as the Winter Olympic Games, there will be fake digital currency illegally manufactured. The anti-counterfeiting of digital currency is very important. Cryptography can be used to realize the anti-counterfeiting and anti tampering of data currency. The central bank's currency issuing center uses the private key to sign the issued digital currency, records the currency generation and transaction flow, and timely feeds back to the central management system.

Asymmetric encryption algorithm can be used for data encryption. Each node in the blockchain has a unique key pair: the public key is public, indicating the identity of the node; the private key is not public, indicating the control of information. Information encrypted with one of the keys can only be decrypted by the corresponding other key. Elliptic curve encryption algorithm is a classical asymmetric encryption algorithm. Its equation is shown in Formula 1.

$$y^2=x^3+ax+b(mod\ p) \tag{1}$$

where $a$ and $b$ are coefficients, $p$ are prime numbers greater than 3, and $G$ (x, y) are discrete points on the finite field $F_p$.

Elliptic curve has the following characteristics: given a certain point $G$ of elliptic curve, it is easy to find the point $kG$; on the contrary, if the point $G$ and point $kG$ are known, it is very difficult to find $k$. In practical application, the asymmetric encryption can be realized by using $k$ as the private key and $kG$ as the public key.

### 3.2 Model

Referring to the possible problems and solutions of 3.1 digital RMB in the Winter Olympics, this paper designs a digital currency wallet infrastructure based on blockchain 3.0 framework, as shown in Figure 2. Blockchain 3.0 is a blockchain architecture with more strict access mechanism and authority control. It is oriented to enterprise level application scenarios beyond the scope of currency and finance, represented by super ledger. Digital currency transaction has higher requirements on data security, so it is more suitable to adopt the hybrid architecture with partial decentralization and strict access mechanism. Its supervision can not be completely operated by public nodes. Therefore, this paper adopts the alliance chain structure, and the members of the alliance read and write the blockchain data according to the authorization.

In the digital currency wallet infrastructure, there is no need for consensus algorithm, because the members of the alliance chain are the people's Bank of China and the major commercial banks, which are reliable, so there is no need for fault-tolerant algorithm and voting to reach consensus. Among them, only members on the chain have the right to account in the blockchain. When a new transaction occurs, the consensus node can generate blocks, that is, bookkeeping in the blockchain. It is supervised by the central bank.

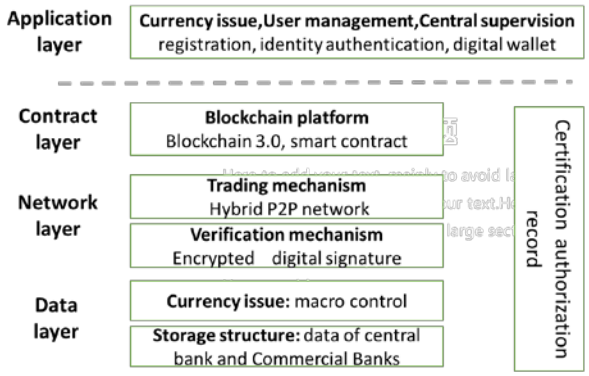


**Fig. 2.** Digital wallet infrastructure based on blockchain.

Centralized background database has great risk. Physical damage of database and communication problems between database and external terminal will lead to database failure. At the same time, excessive centralization will produce asymmetric information,

which may damage the interests of participants and other parties in the market. Distributed storage is a subversive feature of blockchain technology. The management and control of hierarchical structure no longer exist in the system, but through the micro interaction and competition game between network nodes to realize the system operation, which ensures the openness, transparency and authenticity of information, and makes the efficient and large-scale information interaction become a reality. Considering the regulatory requirements of the central bank on digital currency, the transaction mechanism adopts hybrid P2P network to realize the distributed storage of data, as shown in Figure 3.

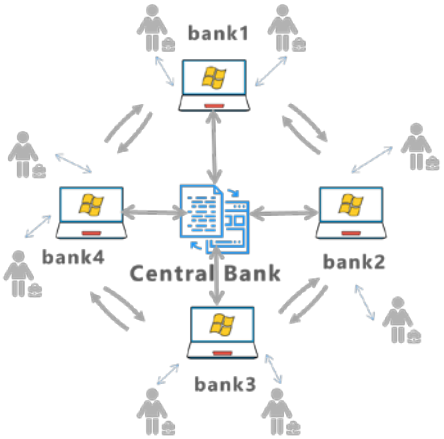


**Fig. 3.** Digital currency transaction mechanism of "partial decentralization". The system is composed of multiple independent nodes, which is like a public account book for members in the alliance chain, each node can keep accounts and audit accounts, but no single node can independently control the account book, all nodes participate together, and constantly update the account book according to strict rules and public agreements. All the data in the system can not be tampered with or forgeable by means of cryptography, and stored in data blocks safely.

The main process is as follows:

(1) When a new transaction is generated, the sender of the message will broadcast the transaction information in the whole network.

(2) The receiving node checks the received data records, and then assembles the data records into blocks.

(3) If and only if the transactions contained in the block are valid and have passed the verification of the institutions in the blockchain, other institutional nodes will recognize the validity of the block.

(4) After receiving the block, other nodes will put the block into the blockchain for storage, and create a new block at the end of the block to extend the chain of the whole block.

## 4 Conclusions

Although the technical feature of blockchain is that it does not rely on the central organization, it does not mean that it can not be incorporated into the existing system of central institutions. As long as it is reasonably designed, the central bank can effectively integrate the distributed operation by using the blockchain to better realize the centralized management and control of digital currency. There is no inevitable conflict between the two. Digital RMB is still in the pilot period, and no one can predict what may happen in the Winter Olympics. The digital currency model proposed in this paper uses blockchain technology in the aspects of transaction mechanism, security and data storage. Blockchain itself is a good technical framework. It is applied to the digital currency of the central bank.

By using its technical advantages of distributed storage, security and trustworthiness, tamper proof and other technical advantages, the digital currency management can be realized with lower cost and higher efficiency. Under the blockchain architecture, the road of digital currency will be wider and wider.

This work was supported by the National Social Science Foundation of China (18ZDA309), the National Natural Science Foundation of China (71531012, 62072463), the Natural Science Foundation of Beijing (4172032), and the Project of Beijing Academy of Capital Development and Strategy Renmin University of China.

## References

1. S. Cheng. Blockchain enabling digital RMB. Financial Expo (Fortune), 40-44(2020)
2. X. Liang, X. You, Y. Xue, F. Xu. *Blockchain: technology and application* [M]. Beijing: China Renmin University Press, (2020)
3. J. Zhang. Design and application scenario of personal credit information sharing platform based on blockchain. Credit reference, **38(10)**:49-55(2020)
4. During the eighteenth collective learning of the Central Political Bureau, Xi Jinping emphasized the importance of the block chain as an important breakthrough in core technology and independent innovation, and accelerated the development of technology and industry in block chain.(2019) https://www.chinanews.com/gn/2019/10-25/8989547.shtmlm
5. J. Sun, Y. Wang, Y. Shi. Blockchain technology and the development of central bank digital currency. Smart China, 60-63 (2020)
6. R. Oliver, S. Stefan. Libra Project: Regulators Act on Global Stablecoins. (2020), **55(6)**:392-398