IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 9, 2021, accepted March 23, 2021, date of publication April 5, 2021, date of current version April 13, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3071033*

# A Hybrid Model for Central Bank Digital Currency Based on Blockchain

**JINNAN ZHANG, RUI TIAN, YANGHUA CAO, XUEGUANG YUAN, ZEFENG YU, XIN YAN, AND XIA ZHANG**

Institute of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China

Corresponding author: Jinnan Zhang (zhangjinnan@bupt.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61774021 and Grant 61911530133, and in part by the Fund of State Key Laboratory of Information Photonics and Optical Communications through the Beijing University of Posts and Telecommunications, China under Grant IPOC2019ZT07.

**ABSTRACT** With the development of blockchain technology, the research on digital currency is attracting more and more attention, especially Central Bank Digital Currency (CBDC), which plays an important role in national economic construction. However, compared with existing cryptocurrencies, CBDC needs a more controllable decentralization and more emphasized supervision. Therefore, the critical part of CBDC is the network architecture that saves computing resources, the technical scheme that is in line with economic ecology, and efficient consensus algorithms. In this paper, we propose a hybrid blockchain system with a modularity network for CBDC. The account scheme is used to record frequently circulated digital currencies, especially for massive small payment transactions when the digital assets and smart contracts with large value fluctuations and weak liquidity are recorded using the Unspent Transaction Output (UTXO) scheme. In terms of network architecture, a modular blockchain architecture is proposed, and a sliced data storage solution is designed to enhance the concurrency of this structured network. We also proposed a CBDC supervision mode for blockchain, and on this basis, the DPOS-BFT algorithm is optimized, which reduces the two rounds of consensus of the original algorithm to one round. Finally, three simulation experiments on scheme, network, and consensus are carried out, which show this system can comprehensively improve the transaction processing and the consensus speed.

**INDEX TERMS** Central bank digital currency, blockchain, consensus mechanism, modular architecture, prototype system.

## I. INTRODUCTION

Virtual currency refers to a formless currency, which is an alternative payment method rather than legally mandatory [1]. Central Bank Digital Currency (CBDC) is a virtual currency based on node network and digital encryption algorithm issue by a country with which has a Legal Credit Protection [2], [3]. In 2008, Satoshi Nakamoto proposed the encrypted digital currency ''Bitcoin'' [4], which is the first fully distributed digital currency [5]. After that, digital currencies such as Bitshares [6], Bitcoin Cash [7], and Dash [8] appeared one after another. Compared with traditional cash currency, digital currency is more convenient to use, lower in cost, and richer in functions [9]. Thus, in the current era of electronic payment, the development of digital currency is the general trend [10]. However, private digital currencies cannot be directly applied at the national level, either in the design concept or performance scheme [11]. Currently, more and more countries have begun to research the CBDC because of the advantages such as payment optimizing, supervision strengthening, and economic output improving. Supported by blockchain technology, CBDC is expected to become the main currency and infrastructure in the new economic era, and play an important role in the financial fields of auditing, banking and insurance [12].

In 2014, China started research on fiat digital currencies and achieved staged results in key parts such as theory and framework. The Bank of England proposed the world's first central bank digital currency in 2015, RSCoin [13]. The prototype is based on the UTXO but does not take into account the legal digital issuance and circulation. In 2016, X. Zhou proposed the technical route and design principles of legal digital currency and pointed out that digital currency needs to be convenient and secure to strengthen the operation and

The associate editor coordinating the review of this manuscript and approving it for publication was Kashif Saleem.

transmission of monetary policy. Canada launched the Jasper project to study the Canadian dollar fiat digital currency in 2017 [14]. In the same year, the Monetary Authority of Singapore, European Central Bank, and Bank of Japan also carried out research on CBDC with the project named Ubin [15] and STELLA [16]. Tsai *et al.* proposed an account-based fiat digital currency in 2018 [17]. They point out that the account scheme has sufficient advantages over the UTXO scheme in performance, and has performed a detailed analysis of the technical implementation. And the People's Bank of China published a prototype system of digital currency and related experimental reports [18]. Ubin and Jasper's project team cooperated with the Bank of England to develop an official digital currency cross-border settlement system in 2019 [19]. And Facebook announced the issuance of Libra, a global sovereign digital currency [20].

To sum up, all countries are scrambling to study CBDC at present, but most of the research is limited to a certain part of the problem. However, a complete theoretical system and innovative technical model are needed for the research and implementation of CBDC. Our solution is a comprehensive and in-depth design of the operating mechanism (issuance and circulation), network architecture, and consensus algorithms. We proposed a network architecture that divides the blockchain nodes into ordering nodes, verification nodes, and central nodes in [21]. Although consensus mechanism was improved base on PBFT, it has not been verified by experiments.

The following contributions are made in this paper: We propose a CDBC scheme with a hybrid technology route. In this solution, an account scheme is used to record frequently circulated digital currencies, especially for the settlement, verification, and inquiry of massive small payment transactions, which can greatly improve the processing speed. It uses the form of UTXO to record digital assets with large value fluctuations and weak liquidity to improve the availability of digital currencies. CBDC's need for efficient payments is met through improvements to the modular alliance chain architecture. The rate of consensus is greatly improved through the improvement of the DPOS-BFT algorithm.

## II. PROBLEM ANALYSIS

To study the problems existing in the current CBDC system, we made analyses from three aspects: digital currency expression, network architecture, and consensus mechanism.

### A. ANALOGY OF CURRENT DIGITAL CURRENCY EXPRESSION SCHEMES

There are two major digital currency expression schemes: UTXO and Account. UTXO is an encrypted string with face value which seems as cash, and the scheme is used in Bitcoin [22]. The transfer mechanism of UTXO is shown in Fig. 1. One or more UTXOs be consumed by a transaction as an input, and several new UTXOs which can be used in a future transaction will be created. UTXO allows multiple transactions in parallel because there is no account. It also has a high degree of privacy and is suitable for currency systems with high-security requirements [23]. Except for Coinbase transactions, the input of a transaction is always linked behind a UTXO. Transactions cannot be replayed, and the order and dependencies of transactions are easy to verify, and whether transactions are consumed is also easy to prove.

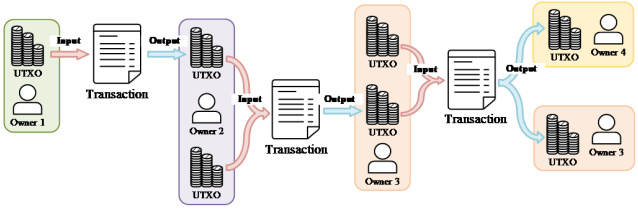


**FIGURE 1.** The transfer mechanism of UTXO.

The account scheme uses a list to save the balance of users like bank accounts. A transaction is valid if the sending account has enough balance to pay for it, in which case the sending account is debited and the receiving account is credited with the value. The scheme is used in Ethereum, the account of which not only saves the balance but also saves the code of smart contract and some internal states when the UTXO scheme saves them in the encrypted string. Account schemes have advantages in transaction processing speed without complicated operation mechanism. And its smart contract have more functions but more complexity or greater resource consumption.

#### 1) THE UTXO SCHEME

We find some problems when applying the UTXO scheme to CDBC, such as high spatial complexity caused by massive small payments. UTXO digital currency relies on transaction records [24]. The input and output of each transaction are UTXO, so the metadata stored in the database is the transaction record. From the metadata, we can derive each UTXO. If the owner provides the correct public key, we can verify the legitimacy of the UTXO. But the calculation of UTXO derived from metadata is quite complicated, especially for a fiat digital currency system with tens of millions or even hundreds of millions of users, there can be billions of transactions in one month. According to data from the China National Network Clearing Corporation, the number of online fund payment transactions from January 24 to 30 during the Spring Festival holiday in 2020 will reach 4.919 billion.

Just searching out so much transaction data as input and output for UTXO imposes a great burden on its server performance, let alone checking the legality within the irreversible cycle of the blockchain. Thus, the UTXO solution cannot deal with such billions of large-scale small-payment simple transactions.

#### 2) THE ACCOUNT SCHEME

More complex contract code requires more storage and runs more resources, and thus it is more likely to cause errors on the system and the network. Running a large number of DApps increases the maintenance cost of blockchain, and it

can be easily crowd out the most basic payment functions of digital currencies. Overall, UTXO also has this shortcoming, due to different operating mechanisms. Its severity is much less than that of the account scheme. Thus, we need a balanced solution which limits the complexity of smart contract when using the account scheme.

In terms of construction and maintenance, the costs of account scheme are higher than the UTXO costs. When it comes to the functionality and scalability, the UTXO is appropriate for building digital assets, and the account is suitable for building DApps. Considering transaction efficiency, the account scheme is better than UTXO, while some flexibility of smart contract are sacrificed.

### B. CURRENT BLOCKCHAIN NETWORK NODE ARCHITECTURE

The blockchain network architecture is divided into traditional peer-to-peer networks and structured modular networks [25]. The former is used in most digital currencies such as Bitcoin, when the latter is used as alliance chains.

#### 1) TRADITIONAL BLOCKCHAIN ARCHITECTURE

Traditional digital currency systems tend to use a unified wallet software as a node carrier, which updated by a community or cooperative organization and keeping all nodes in a fair state. Hence, a node usually keeps a complete ledger database and receives digital currency rewards from local mining. Besides, the node also stores the user's private key, initiates a transaction, acts as a proxy for others, and provides basic functions (consensus, encryption, decryption, hash operations, transaction pools, etc.). Therefore, all nodes in the architecture are comprehensive but difficult to make custom optimization.

Users and enterprises interact by transactions, especially from the Dapp contract. In a peer-to-peer network, the transaction sent to the blockchain using a broadcasting way. Due to this, multiple nodes may independently process the same transaction request at the same time. But according to consensus rules, only one node can obtain the accounting opportunity in a period. Therefore, the processing of this transaction by nodes without accounting is meaningless.

In general, it can be known that the traditional digital currency system architecture has the following problems:

a) Waste of node resources. For the beginning, the participants mortgage their computer resources to obtain profits. These profits were invested to improve the system performance. But the relationship between the nodes is competitive, the nodes cannot cooperate and independently handle the repeated transaction. All the resources cannot be fully utilized either.

b) The lack of modularity. All the functions of digital currencies are integrated and carried out by official publishers. The participants need to use a fully developed official node program. It is difficult to allocate or modularize node functions according to the advantages of computer resources in their possession, which makes it impossible to apply distributed solutions like microservices. Therefore, performance, compatibility, and security may become hidden issues in the future.

c) The competition of transaction processing fees is contrary to the design concept of CDBC. In a system with limited performance, users need to pay more fees to ensure their transactions be prioritized. This is inconsistent with the social fairness required by CDBC.

#### 2) MODULAR BLOCKCHAIN ARCHITECTURE

As the alliance chain itself is used in a semi-centralized scenario, the nodes have more credibility between peers. The architecture design of alliance chain is more flexible, such as the Hyperledger Fabric [26]. Especially, this architecture modularizes the functions of nodes and sets different permissions for them. When a fault occurs, the faulty part can be repaired separately in this way. If there is a demand, a type of node can be expanded alone to enhance the processing capacity. In the design, the repeated processing work is reduced, more resources are saved, thus the performance of the system is improved.

There are still several problems in this architecture. Firstly, the current using alliance chain network is mostly designed to share data between business organizations across industries. In order to improve business richness, all functions in the chain are based on smart contracts, including simple transactions. Although we can implement all the demands of CBDC by smart contracts, the system's performance and scalability are inferior to those of directly processing on the basic function. Secondly, the solution for permissions in the alliance chain is using a method similar to build several subchains. It uses nodes with different permissions to maintain different blockchains with the same architecture [27]. The design does not fit the CDBC that needs to be unified.

Compared with the centralized system, the traditional digital currency architecture has the drawbacks of operating efficiency and resource consumption. The modular architecture has excellent performance, but its original design concepts do not fit the CDBC reformed.

### C. CONSENSUS MECHANISM IN THE CURRENT BLOCKCHAIN

The consensus mechanism is the core of the blockchain system telling how the nodes synchronize the ledger. Most of the components of the blockchain architecture are designed around the consensus mechanism to ensure that the system can still operate normally under any extreme conditions. Common consensus mechanisms include Proof of Work (POW), Proof of Stake (POS), Practical Byzantine Fault Tolerance (PBFT), Ripple Consensus Protocol (RCP), Delegated Proof of Stake (DPOS), and so on.

#### 1) THE POW CONSENSUS MECHANISM

The POW mechanism is designed for the Bitcoin system. The computing power competition of distributed nodes is used to ensure the consistency of data and the security of consensus.

The nodes on the POW network compete for ledger writing via complex and meaningless calculations. The network can keep stable, except for some nodes own half of calculation ability. To solve the problem of block forks, the period of producing each block cannot be too short. But this can cause a decrease in transaction processing speed.

#### 2) THE POS CONSENSUS MECHANISM

In POS-based cryptocurrencies the creator of the next block is chosen via various combinations of random selection and wealth or age (i.e., the stake). The ledger writing authority is easier obtained by the node with the higher stake. The bookkeeping nodes do not need to run complex calculations, which effectively avoids resource consumption. But the nodes can get the bookkeeping authority are always those who have the most mortgage stake. Accordingly, there is a potential risk that the network is controlled by the richest node. Similar to POW, to solve the hard block fork, the transaction processing efficiency of the blockchain system is still relatively low.

#### 3) THE PBFT CONSENSUS MECHANISM

PBFT is a relatively balanced solution, which can be stable when the number of all nodes is at least $3f+1$ (f is the number of nodes that do not respond to failures/faults). However, theoretically, the nodes need to perform $2n^2+n$ (n is the number of nodes) times of communication to consensus, which is not efficient enough when n is very large. But this mechanism is still faster than POW and more secure than POS.

#### 4) THE DPOS CONSENSUS MECHANISM

DPOS consensus algorithm is improved based on the POS algorithm, which used in Bitshares, Steem, and EOS. The scope of block producer 's nodes is greatly reduced, and these master nodes mortgaged their currency or computer resource to get the vote from the entire network. A small-scale POS or PBFT consensus is used between these master nodes to synchronize and broadcast blocks. Due to the number of producer nodes generally is less than 50, the broadcast numbers and resource requirement is reduced, and the processing speed is improved. However, there are some considerations: Firstly, for the normal users, the enthusiasm for voting is not high, the risks of Sybil Attack should be considered. Secondly, the DPOS used in EOS point that the block fork is easy to appear in a high latency network, which requires more additional measures to solve. Therefore, in extreme cases, the performance of DPOS may be worse.

In the POW and POS consensus mechanism, most of the participants only verify the produced block, but cannot refute the block content when the malicious nodes have controlled half of the resource or vote. The PBFT mechanism is stable and efficient, but the performance can severely decrease when the number of nodes continues to increase. DPOS is a balanced mechanism to solve the Sybil Attack when used in a relatively centralized environment such as CDBC. Besides, we also consider to use the DPOS-BFT algorithm that combining the PBFT to further improve the processing speed.

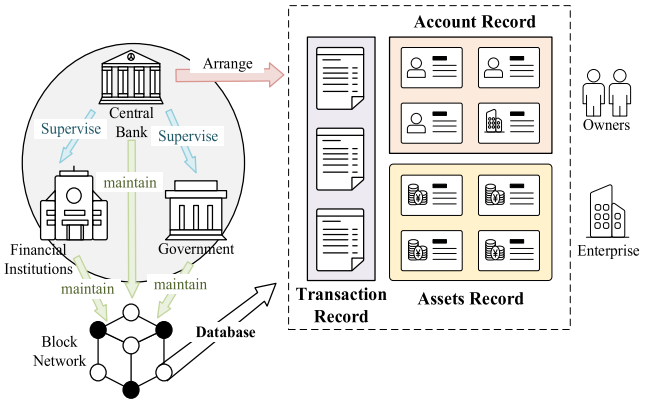


**FIGURE 2.** The hybrid digital currency scheme.

## III. THE SCHEME OF CBDC

### A. OVERALL DESIGN

UTXO and account are two basic digital currency scheme models. Some defects were found when these models are directly applied to CBDC as analysis in the previous chapter. In this section, a hybrid digital currency scheme is proposed to mix the advantages of the two schemes.

The hybrid digital currency scheme is shown in Fig. 2. The bottom layer of the solution uses a distributed blockchain network formed by various commercial and government departments under the leadership of the central bank. The account scheme is used for the calculation and representation of digital currency to accelerate the basic transactions. In order to meet the additional function requirement such as financial assets and Dapps, we implement them with UTXO scheme. This can make up the limitations in the smart contract of the account scheme without hindering the processing of basic transactions.

According to the "Analysis Report of China's Fund Industry in 2020", "Overall Situation of the Payment System Operation in the Second Quarter of 2019" [28] and "Statistical Report on the Development of China's Internet Network in 2019", it is estimated that 87% of online transactions are small payments Class operation, no need to extend special functions. Therefore, the basic payment transactions should be ensured to run in the highest priority without any barriers. In our design, the digital currency for payment with frequent circulation and stable value are recorded in the account scheme. While the financial assets are recorded in the UTXO scheme with a complex contract, large value fluctuations, and weak circulation. By this mean, the advantage of payment processing speed in the account scheme can be given full play, because the most resource-consuming operations such as contract and assets are independently processed in the UTXO scheme.

### B. DESIGN OF KEY MODULES

#### 1) ACCOUNT

In the account scheme, the amount of digital currency owned by the user is represented by his account balance. The account is completely visible to its holder, and also transparent to

**TABLE 1. The structure of account, asset, and transaction.**

| Account | Asset | Transaction |
|---|---|---|
| id | id | id |
| timestamp | timestamp | timestamp |
| operates | operates | type |
| address | type | sender |
| publicKey | owner | receiver |
| value | issuer | value |
| contracts | value | input |
| exFunc | contracts | output |
| | exFunc | signatures |
| | | contracts |
| | | exFunc |

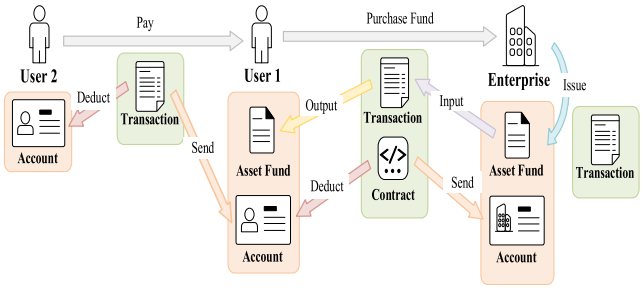


**FIGURE 3. The schematic diagram of the transfer mechanism.**

the central bank. Other nodes and third parties cannot obtain the user's private information. Users need to submit relevant personal or financial department information for account approval. Meanwhile, a user can only hold a limited number of accounts according to the law of the central bank.

The design of he account structure in Java class expression is shown in Table 1. Among them, *id* is the unique identification of the account. *Timestamp* is the last modified time. *Operates* cites all the related transactions of this block to improve the trace speed. *Address* is the identity of the owner. *PublicKey* is the public key of the account. *Value* is the balance of the account. *Contracts* storage all the lightweight executable functions of account smart contract, which standardized by the central bank and can be quickly executed with light resource consumption unlike the digital assets or UTXO contract developed by the third parties.

#### 2) DIGITAL ASSETS (UTXO)

The digital asset is an electronic voucher with the UTXO scheme for a right that requires others to pay digital currency in our design. It can be used as bank savings, securities or funds, etc. The transferability and tradability were endorsed by the central bank. In the UTXO solution, a digital asset is a set of strings that encrypt the basic elements of the asset. The basic elements are the key information such as the ownership, face value, and smart contract constraints of the digital asset.

The design of the asset structure in Java class expression is shown in Table 1. *Id* is the unique identification of a digital asset. *Timestamp* is the creation time. *Operate* cites the origin transaction which outputs this UTXO. *Type* expresses the nature of this digital asset. *Owner* cites the account right to use this UTXO. *Issuer* storages a verifiable publisher 's Information. *Value* is the amount of this digital asset. *Contracts* storage all the unlock scripts or smart contracts of the digital asset which is implemented by the issuers and may have complex functions or limits and consume lots of resources.

#### 3) TRANSACTION

Transactions are the basis for the changes of user accounts and digital assets. There are different types of transactions not only to transfer digital currencies or assets but also to run smart contracts. For the input of UTXO or the digital currency amount, receiver and sender should be written in the transactions. Besides, each transaction must carry the signature of the owner of account or assets to prove the validity.

The design of the transaction structure in Java class expression is shown in Table 1. *Id* is the unique identification of a digital asset. *Timestamp* is the processing success time. *Sender* and *receiver* are the initiators and target account of the transaction. *Value* is the amount of digital currency or the number of assets for transfer. *Input* and *output* cite the id of UTXO supported. It needs to be noted that input should be provided by the sender before processing when the output is created by the operator. *Signatures* storage all necessary digital signature from the sender. *Contracts* storage the lightweight smart contracts or scripts the same as the account scheme, which provides some convenient operations but not consume lots.

### C. DESIGN OF THE OPERATING MECHANISM

#### 1) TRANSFER MECHANISM

The transfer mechanisms for digital currency or digital asset are different owing to mixing the account and UTXO in our design. The mixed transfer mechanism in the typical scenarios is shown as Fig. 3.

For the digital currency payment scenario where user 2 pays a digital currency to user 1, the process is as follows: First, user 2 needs to specify the consumption amount, and transfer account by digital currency wallet software or other enters. After that, the wallet automatically generates a transaction according to the instructions and sends it to the CBDC network that finally transfers it to the corresponding node for operation. The node can recognize the payment requirements and verifies its legitimacy. At this time, if there are no active smart contracts under the accounts of both parties, the payment process is started directly: the account of user 2 is deducted, and the account balance of user 1 is increased. The transaction and account change can be written in block. After the next blockchain cycle begins, transactions become irreversible. Finally, user 1 makes a query or accepts the push information from the wallet to confirm the successful payment.

For the digital asset trading scenario where user 1 wants to buy a fund from a financial company, the process is as follows:

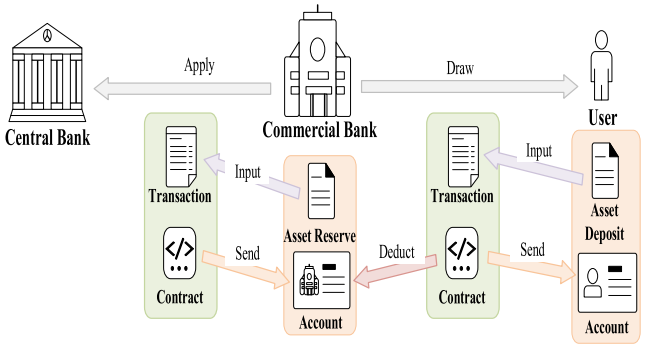


**FIGURE 4.** The schematic diagram of the issuance mechanism.

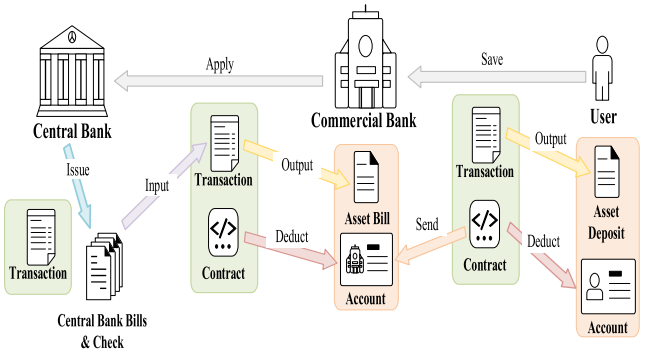


**FIGURE 5.** The schematic diagram of the withdraw mechanism.

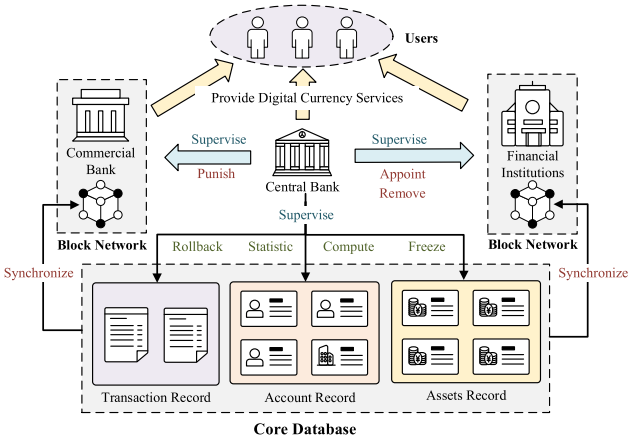


**FIGURE 6.** The "single-core" supervision mode.

First, the fund needs to be issued as UTXO by the company. After user 1 negotiating purchase with the companies through websites or dealers, a transaction to pay for digital currencies and transfer UTXO is created. Both user 1 and company sign the contract with their private key, and the generated signatures are attached to the transaction, which are used as the validity verifying parameters. After the two parties confirmed that, the transaction is sent to the CNDC network. After these signatures checked by the third-level nodes, the account of user 1 is debited, and the company's account balance increases. Then the input fund UTXO from the company is cancelled, while the fund UTXO owned by user 1 is generated. If there is an overflow in the input fund UTXO, an additional fund UTXO owned by the company is generated as a change, and the amount is the overflowed part.

### 2) ISSUANCE, CIRCULATION, AND WITHDRAWAL

The issuance of CBDC is similar to the UTXO transfer. As shown in Fig. 4, here is an example that a commercial bank withdraws the reserve from central bank: First, the commercial bank applies, then a special transaction is generated after approval. The transaction does not specify the sender but carries the signature of the central bank. If the commercial bank held a CBDC reserve of digital assets, it can use them as input for transactions. Otherwise, it converts cash reserve into CBDC reserve. After that, the transaction sends the corresponding amount of digital currency to the account of the commercial bank, whose reserve is deducted on a reserve manager non-CBDC system in the central bank. In the next blockchain cycle, these transactions are synchronized to the entire network, thereby completing the issuance of digital currencies.

As shown in Fig. 4, The circulation of CBDC is mainly through users' savings and withdrawals. In fact, the deposits can also be regarded as a UTXO asset used for the input of transactions. When saving money, commercial banks also provide users with UTXO deposit through the output of transactions as the proof of saving.

Fig. 5 shows the design of the CBDC withdraws. First, the central bank issues a certain amount of UTXO bills or checks, and commercial banks apply the purchasing authority of them. At the time of purchasing, the UTXO bill is used as the input of the transaction, and the smart contract of the bill deducts the account of the commercial bank. Finally, the commercial bank owns the output UTXO bill to complete the withdrawal of digital currency.

### 3) SUPERVISION MODE AND SECURITY

We adopt the "single-core" supervision mode supplemented by the alliance chain [29]. The supervisory mechanism is shown in Fig.6. The central bank supervises the data of the blockchain network and punishes or appoints nodes. All nodes should hold digital certificates issued by the central bank. Whether the third-party companies and financial institutions want to issue digital assets, or participate in CBDC accounting, they must apply to the central bank for digital certificates. In addition, the central bank has the right to freeze the illegal accounts, roll back transactions, and confiscate assets or CBDC.

Besides, the data of peer nodes are transparent to each other has the same privilege, and the final approved data is expressed on the blockchain network for preventing the central bank's misuse operation. The mandatory operation executed by the central bank firstly should be broadcasted to the most privileged node which storage the blockchain data. Nodes verify and assess the operation, and can make a refusal when the central bank is being controlled or attacked. Due to the characteristic of the consensus algorithm, the attacker needs to control the central bank and most of the node, otherwise, the network can correct errors itself. Relatively, if the attacker has controlled most of the nodes exclude the

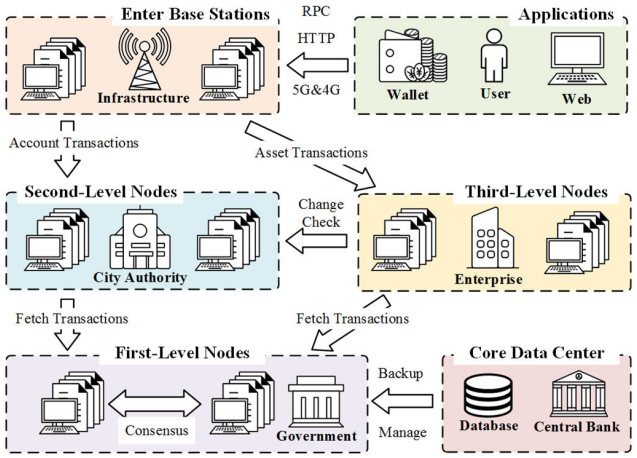


**FIGURE 7.** Overall architecture.

central bank, the central bank can also use its mandatory operation to check and balance the attacker, finally fixs the data after nodes being restored.

## IV. NETWORK ARCHITECTURE

The traditional digital currency architecture generally has the problems of insufficient operating efficiency and excessive resource consumption. Thus it is not suitable for CBDC that requires high throughput. The high-efficiency blockchain architecture represented by the alliance chain has excellent performance and modular architecture. But its application scenarios and some design concepts are not compatible with CBDC. Therefore, the architecture design proposed in this paper is optimized based on the alliance chain.

A customized structured and modular alliance chain architecture for CBDC is proposed as the network layer. Different from using the unified wallet in traditional blockchain architecture, nodes are divided into types in our design. They are responsible for consensus, account processing, and UTXO processing. To improve the concurrent processing capability, a sliced storage solution is proposed to optimize the data management, and the working scope of nodes with the same type are independent and concurrent. This part is introduced in the next chapter.

### A. OVERALL STRUCTURAL DESIGN

The overall architecture design principles are as follows:

1) The architecture should strengthen the regulatory nature of digital currencies so that central banks and governments can conduct data accounting easily.

2) The architecture must have efficient transaction processing capabilities, especially to ensure the conduct of basic payment transactions.

3) The construction difficulty and cost of the architecture cannot be too high.

Based on the above principles, the digital currency architecture designed in this article is shown in Fig. 7. The architecture adopts a modular idea and divides the system into six levels, application layer, enter layer, third-level node, second-level node, first-level node, and core data center. The application layer is the entrance of the transaction, which consists of users, operable wallets, and web interfaces. It sends the generated transaction requests to the entrance layer through RPC, HTTP, 5G and other methods. The enter layer is composed of some urban infrastructure, base stations, and agent nodes. It is responsible for distributing transactions, especially account transactions to secondary nodes, and asset transactions to tertiary nodes. The second-level node is composed of special nodes maintained by the city and state-level information departments, operators, etc. It is mainly responsible for the processing and sequencing of account transactions. The third-level node is composed of commercial banks, digital currency application provider companies, financial institutions, and network service provider companies. It is mainly responsible for the processing and sequencing of digital asset transactions, and it can be synchronized with the second-level nodes at any time. The first-level nodes are mainly maintained and managed by provincial governments. It is responsible for block production and data consensus. The core data center does not participate in the operation of the blockchain. It is mainly responsible for backing up, supervising and saving the final valid data, and managing the first-level nodes.

### B. THE MODULAR DESIGN OF THE ARCHITECTURE

According to the above analysis, our architecture does not use the fully quantized node method of traditional blockchain but divides it into six levels based on the modular idea. This allows maintainers to deploy equipment as needed at all levels. We introduce each level in the architecture in detail below.

#### 1) APPLICATION LAYER

The application layer directly contacts with users. It is a kind of digital currency transaction application software running on electronic devices, for instance, mobile phones and computers. The application layer is usually used as a wallet in the blockchain, which is responsible for key management, signature, transaction generation, and some other functions. In this design, considering the security and applicability of digital currency, we divide wallets into official wallets and third-party wallets. The official wallet contains private key management and encryption implementation. It must further call the interface of the official wallet for the actions need to call the private key or the identification information of users, which include signing, verification, and other actions in the third-party wallet. Its structure and function are shown in Fig. 8.

#### 2) ENTER LAYER

The enter layer consists of communication infrastructures such as switches and servers. It is mainly maintained by equipment suppliers and network operators. The architecture of the enter layer is shown in Fig. 9. The enter layer does not participate in transaction settlement and data maintenance. Its main functions include: ① Pre-checking the submitted

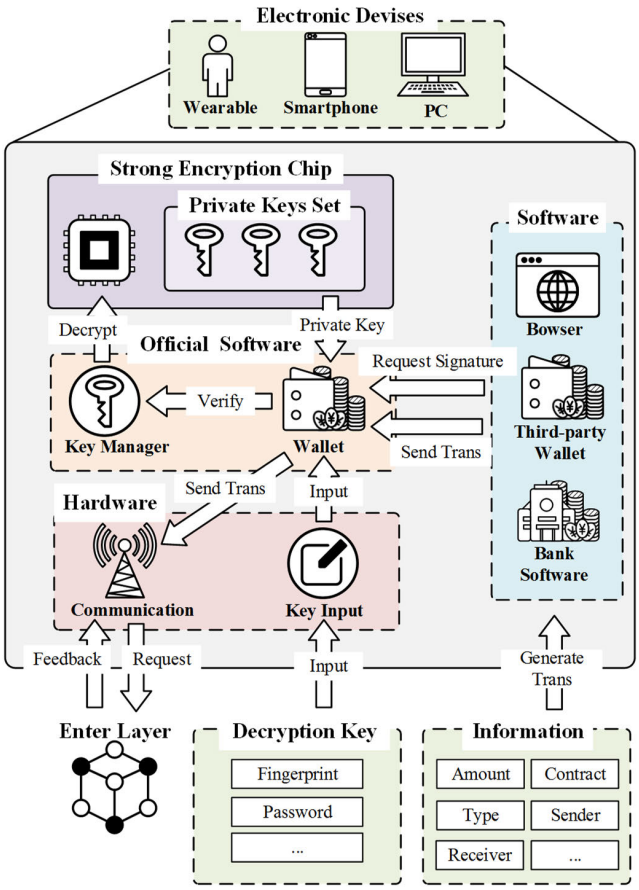


**FIGURE 8.** Application layer architecture.

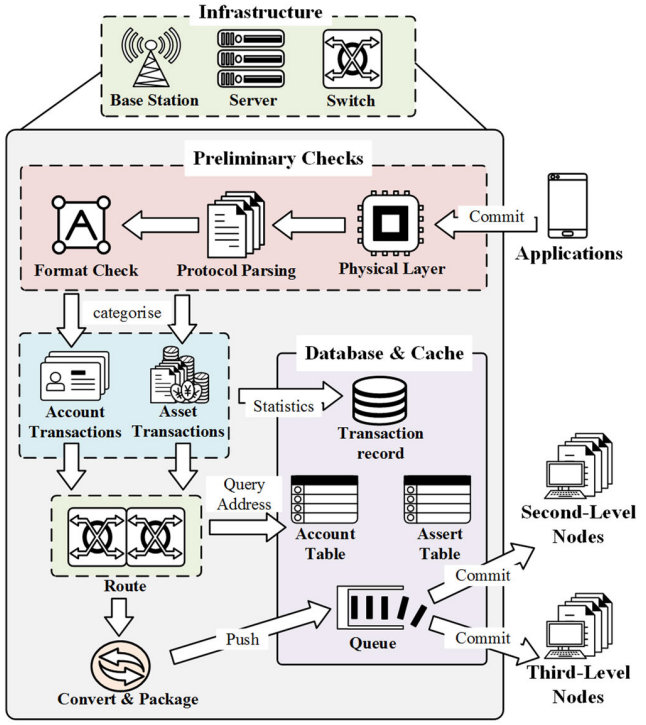


**FIGURE 9.** Enter layer architecture.

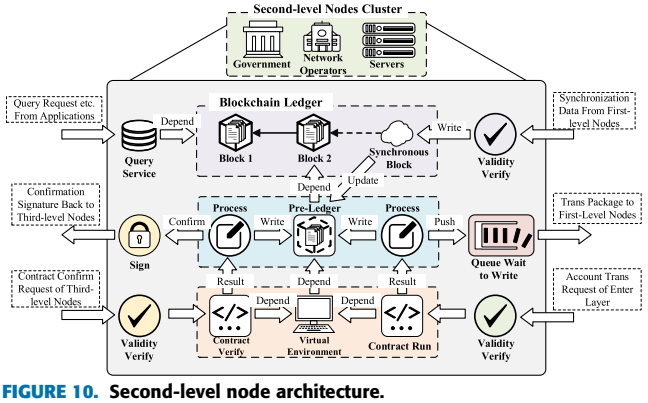


**FIGURE 10.** Second-level node architecture.

transaction to repair the loss in communication and ensure the format and protocol are correct; ② Sorting the second-level nodes and the third-level nodes with different responsibilities, and ensuring the load balance of the nodes in the large-scale transaction scenario. ③ Making preliminary statistics on the transactions submitted in the network, recording and limit the number of repeated transactions.

### 3) SECOND-LEVEL NODE

The second-level node is the core of handling account transactions. It stores all account data and related transaction data in a distributed manner according to the region where users and enterprises are registered. The second-level node is maintained by the local government or officially authorized network operator, Internet service provider, commercial bank, etc. Therefore, the transaction processing scope between different second-level nodes is distinctive. The data recorded by the second-level node is a subset of the main chain's ledger, called the main ledger. However, the second-level node cannot directly rewrite the main ledger. The main ledger can only be updated after the blockchain is synchronized. On other side, the second-level node also records a pre-ledger. The deductions for processing transactions are carried out on the pre-ledger to ensure the node can still process subsequent transactions before the transaction is finally confirmed on the chain.

The overall architecture of the second-level node is shown in Fig. 10. The second-level node needs to receive information from different levels, including service query requests from the application layer, data synchronization and transaction pull requests from the first-level node, account transactions from the entrance layer, and asset transaction information from third-level nodes, etc.

### 4) THIRD-LEVEL NODE

Because the flexible functions of digital assets and the high demand for computer resources, third-level nodes are needed to maintain and manage them for developers. Each digital asset can only be handled by one third-level node. However, data backup can be negotiated between the third-level nodes to ensure data security under special circumstances.

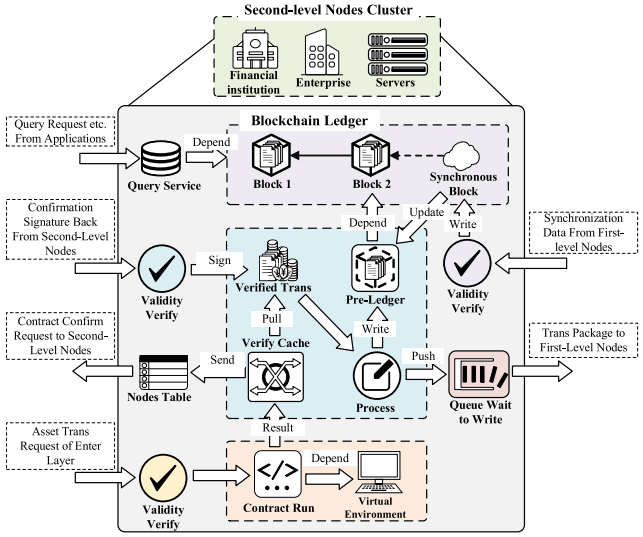


**FIGURE 11.** Third-level node architecture.

The messages that the third-level node may receive from other levels include: ① The query requests from the application layer; ② The data synchronization and transaction pull requests from the first-level nodes; ③ The asset transaction requests from the enter layer; ④ The contract confirmation returned from the second-level nodes. The functional architecture of the third-level node is shown in Fig. 11.

#### 5) FIRST-LEVEL NODE

The first-level node is mainly responsible for the final legality verification of the transaction. The production of the block and consensus does not involve the operation of the transaction. The first-level nodes are operated and maintained by provincial governments or central banks. The primary node maintains complete blockchain ledger data, including all accounts, assets, and transaction records. In particular, the ledger between all the first-level nodes must be consistent, to ensure that the correction is made by the minority in the majority when the fork occurs. Each first-level node administers a large number of second-level nodes and third-level nodes, and is responsible for the data synchronization of subordinate nodes. This hierarchical management model can distribute network pressure and improve the overall performance of the system.

The overall architecture of the first-level node is shown in Fig. 12. First-level nodes need to actively pull account transaction data from second-level nodes, asset transaction data from third-level nodes, transaction group data from other first-level nodes, and consensus information from other first-level nodes.

### C. SLICED DATA STORAGE DESIGN

It can lead to a decrease in transaction processing performance when the UTXO solution is applied to digital assets. And UTXO fragmentation can also generate greater storage pressure. A sliced data storage scheme is used to solve the above problems, as shown in Fig. 13. The design can pre-

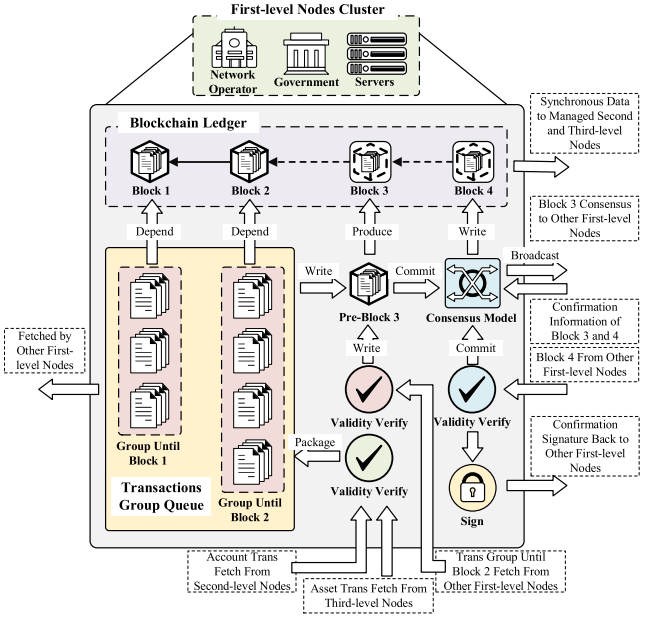


**FIGURE 12.** First-level node architecture.

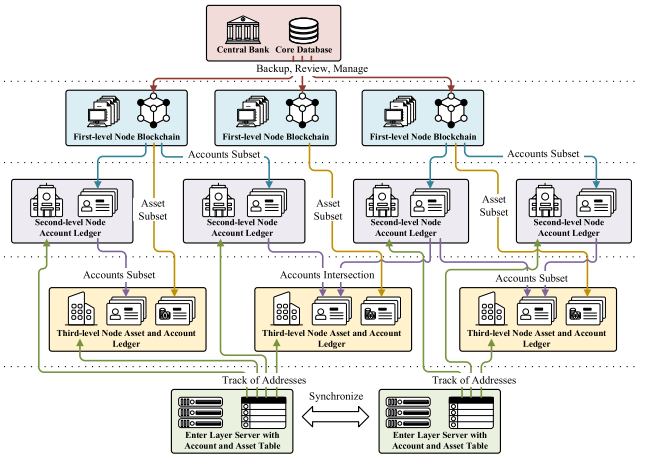


**FIGURE 13.** Data storage scheme.

vent secondary nodes from storing redundant data that is not commonly used in transaction processing, make these non-consensus nodes back up data on demand, and then greatly saving construction and maintenance costs.

In this schema, both the core data center and the first-level nodes maintain a complete blockchain database. The first-level node is the production node of the block. It saves the main chain that performs blockchain consensus and updates every cycle. The core data center backs up the primary nodes asynchronously. When performing data backup, the results recorded on the main chain must be reviewed. When abnormal or illegal records occur, instructions such as freezing and correction must be issued to the first-level nodes. Therefore, the core data center usually lags behind the data of the first-level node, but it is the final valid data. The second-level node only stores account data and related transaction data. The content stored by each second-level node is a subset

of the complete ledger of the first-level node, which is not intersected in theory. So all the second-level nodes have the same functions but different processing scopes. The third-level node only stores the asset data about its operation, the related account data and transaction data. The asset data stored in the third-level node is also a subset of the first-level node's ledger and not intersected with each other. However, the account data stored in the third-level node can be a subset of a second-level node or the sum of multiple second-level node subsets. The design takes into account that digital assets can be held by different accounts across secondary nodes. Under the storage scheme, each transaction can be uniquely processed to a node at a certain time. The server in the entry layer records the processing address of each transaction in the form of a dynamic routing table. It can be assigned to the corresponding processing node, when the transaction passes through the entry layer,.

## V. CONSENSUS MECHAINSM

Considering the disadvantages of the traditional blockchain mechanism and the characteristics of CBDC, we think DPOS and PBFT is suitable for this scene. We tend to use the DPOS-BFT consensus that votes to several block producers consenting with a PBFT way to transfer blocks and determining the order of production. We, therefore, propose a novel consensus algorithm called POA-PBFT, based on the improvement of the DPOS-BFT algorithm. In this section, we introduce the mechanism of the POA-PBFT and the improvement compared with the DPOS-BFT.

### A. POA-PBFT

#### 1) THE ELECTION MECHANISM

We changed the election of the bookkeeping node from voting by all blockchain participants to direct appointment and removal by the central bank. In this way, the voting consumption can be removed, and the position of producers could be more stable to reduce the time of network change. And there is no need for candidate nodes to deploy the producing facilities. Besides, a shutdown node can be replaced by a candidate node immediately in DPOS. In our design, other nodes can temporarily replace the work of the shutdown node.

#### 2) THE BLOCK PRODUCTION SEQUENCE

The production order of the blocks in DPOS is negotiated by all producers and the block number increased freely. In POA-PBFT, however, a certain node specified by the central bank can produce a fixed block number block. When a node is delayed and the next node cannot receive the block, the next node cannot use the number of the delayed block as in DPOS. This can effectively avoid the generation of forked chains.

#### 3) THE PROCESS OF SHUTDOWN

Once a node shuts down and cannot notify all other nodes, the central bank finds the lack of the block accurately when it synchronizes data a few blockchain periods behind the and place them in the local chain.

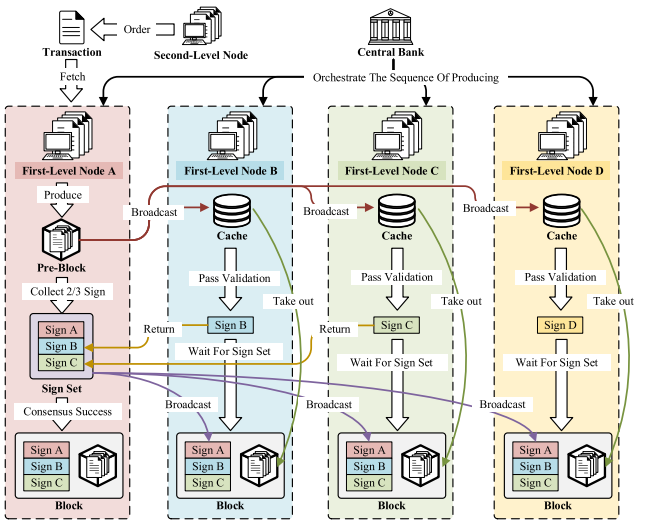


**FIGURE 14.** The operation process of POA-PBFT.

network, and checks the node, and notify other nodes actively. After that, the network eliminates the invalid block number and keep running. Before this node is repaired, other nodes can temporarily replace its work. So the reduction of the processing capability caused by the shutdown can only last for a few block periods.

To solve the fork problem due to delay, DPOS-BFT needs two rounds of consensus [30]. We avoid the fork, and the system performance can only drop for several periods of the block before the central bank checks it in our design. This optimization can remove one round of consensus and almost reduce half of the time consumption.

### B. ANALYSIS OF THE CONSENSUS PROCESS

Fig. 14 shows the consensus process of the POA-PBFT algorithm. Assume that there are four producer nodes A, B, C, and D in the network, the central bank has specified the order of node producing and the block number. At this time, it is the turn of *node A* to produce blocks. First, *node A* packages the transaction groups consist of transactions pulled from the subordinate node before generating the block. When the block is generated, all the transaction groups can be written in a new block. The block is only a pre-block in *node A* and has not been recognized by the network. After *node A* signs the block, it can be broadcast to other producer nodes: B, C, and D. They can first store the block in cache and check the validity. If the verification passes, they can return *node A* their signature of the block. After *node A* collects 2/3 of the node's signatures, the block reaches an irreversible state. After that, *node A* can generate a signature set and broadcast it to others again, and then place the block with the signature into the chain. At this point, the next block period is ready, even if other nodes had no time to write the block. Because there are 2/3 node confirmations on the block of *node A*, the block is legal. After receiving the signature set, B, C, and D verify the

signature set, take out the blocks from the cache and place them in the local chain.

## VI. EXPERIMENT AND ANALYSIS

### A. SECURITY ANALYSIS

The security analysis of the hybrid model for CBDC we proposed mainly includes two aspects: model security and transaction security. Model security is guaranteed by the storage scheme and consensus mechanism. And the operation mechanism and supervision mode we designed can ensure transaction security.

#### 1) MODEL SECURITY

In terms of data storage of our model, the central bank's core data nodes and the first-level nodes keep the complete records of transactions, accounts, and digital assets. The second-level nodes keep the records of transaction and account after data slicing, which are allocated according to permissions. And the three-level nodes save the account data without privacy and the records of assets and transactions about the node operation company. This sliced date storage scheme not only reduces the diffusion of sensitive data but also decreases the redundancy of data storage. Therefore, we can improve the security of the system and also facilitate the central bank's supervision.

At the same time, the POA-PBFT we proposed is still essentially a state machine replication algorithm. It guarantees liveness and provable safety and provides partly fault tolerance. The specific proof process can refer to [31].

#### 2) TRANSACTION SECURITY

Different from the general digital currency, CBDC is not a financial product for speculation. It is used for the whole society rather than a specific community. Therefore, its safety largely depends on the regulatory mechanism.

We adopt the ''single-core'' supervision mode that uses the central bank as the core, supplemented by the alliance chain. The core data center of the central bank is the node with the highest authority. It does not participate in the bookkeeping of the alliance chain, but responsible for the supervision of nodes, including data synchronization and analysis. We demonstrate the details of this supervision mode to ensure transaction security in part III above.

### B. PERFORMANCE ANALYSIS

In order to test the architecture, we implemented a blockchain experimental platform in Java. The platform equipped with a series of minimized blockchain nodes based on different operating mechanisms. It ran on a physical server when all the nodes running in Docker. Communication between nodes used a JSON-based P2P protocol, and the network latency was randomly simulated and could be dynamically adjusted. We used xxHash algorithm and SM2 encryption algorithm in the experiment. Other configurations are shown in the following Table 2.

**TABLE 2. Experimental configuration.**

| Option | Table Column Head |
|---|---|
| Operating System | CentOS-7 (1810) |
| Database | MongoDB 4.0 |
| Programming | Java 11.0.1 |
| Virtualization | Docker 18.03 |
| CPU | Intel Core i5-8250 |
| RAM | DDR4 16 Gb |
| Storage | SAMSUNG KUS030202M-B000 |

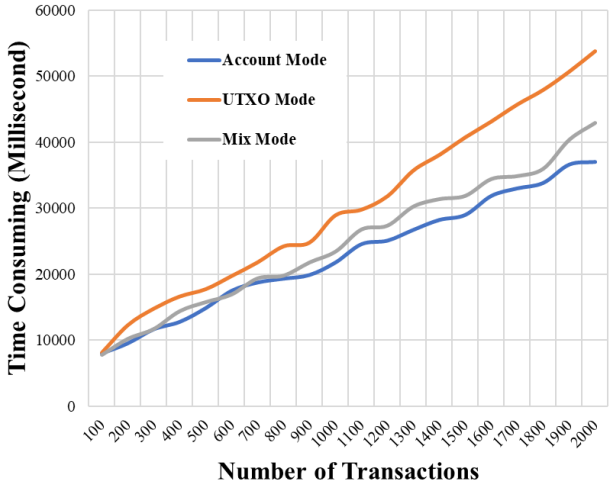


**FIGURE 15. Time consumption of different modes.**

First, We tested the processing time required by three types of nodes (UTXO, Account, and Mixed) when processing-intensive transactions. To ensure that nodes are running at full capacity, intensive transactions are generated by the random transaction generator in a Poisson distribution when the density of transactions can be adjusted based on node's buffer pool load. In mixed mode, the ratio of UTXO to Account is 2: 8, which is higher than the actual situation. The experimental results are shown in Fig. 15. When intensive transactions continue to increase, the processing time of different solutions increases linearly. Under the same conditions, the average time consumption of the UTXO mode is 28.5% higher than that of the Account scheme. The mixed-mode can reduce the average time consumption taken by the UTXO mode by 16.4%. This proves that the performance of the mixed-mode is further improved when the ratio is close to 2: 13 in the real situation.

Next, under the mixed-mode, we tested the time consumption of traditional network architecture and the improved network architecture in processing-intensive transactions. The experimental results are shown in Fig. 16 with the same conditions in the previous experiment. When the number of intensive transactions increases, the processing time of both architectures increases linearly. Compared with the traditional blockchain architecture, the architecture solution we proposed has reduced the average processing time of intensive transactions by about 26.3%.

Finally, we tested the time required for the PBFT algorithm and the POA-PBFT algorithm to complete a round of con-

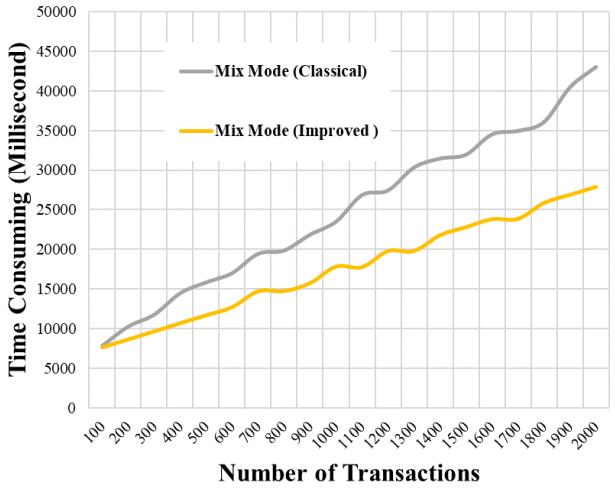


**FIGURE 16.** Time consumption of different network architectures.

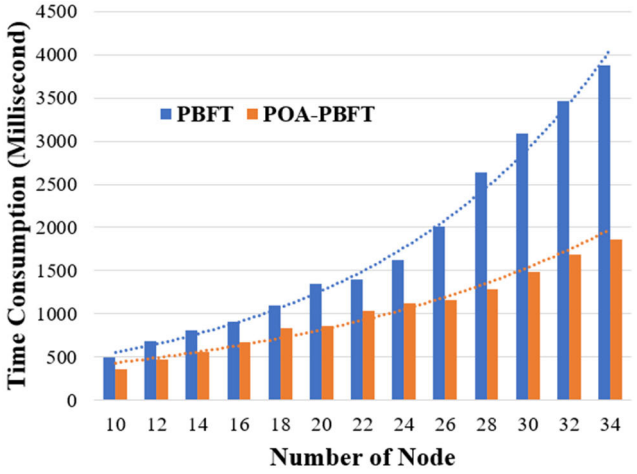


**FIGURE 17.** Time consumption of different consensus algorithms.

sensus under different numbers of nodes. We set the average network delay of nodes to 20 milliseconds. We have made a lot of experiments on a different number of nodes. The abnormal data were eliminated and the results were averaged. The experimental results are shown in Fig. 17. The consensus time of the PBFT algorithm increases exponentially, while POA-PBFT algorithm shows similar linear growth. When the number of first-level nodes is between 30 and 50, the optimization makes obvious improvement. The performance of POA-PBFT algorithm is improved by 51.8% to 64.7% compared with PBFT algorithm.

Experimental results show that mixed-mode can significantly improve processing efficiency while retaining UTXO characteristics, and the structured and modular network architecture can further increase transaction processing speed. At the same time, POA-PBFT algorithm can greatly reduce the time consumption of consensus compared with PBFT.

## VII. CONCLUSION

A hybrid blockchain system for CBDC is proposed, which is innovative in three levels: technology scheme, network architecture, and consensus mechanism. The operation mechanism of the issuance, circulation, and return of CBDC is comprehensively designed in this scheme. This hybrid model of UTXO and account improves the processing rate by 16.4% compared with UTXO. And the transaction processing speed is improved by 26.3% using the network architecture. With the improvement of the consensus algorithm, the consensus speed is improved by more than 51.8%.

There are still some problems to be solved. For example, the implementation of smart contracts and related experiments have not been carried out due to experimental conditions and manpower constraints. Therefore, the optimization effect of smart contracts theory needs to be verified by subsequent experiments. And we didn't study how to use the system for currency regulation and investment at the national policy level. Although it is not a technical issue, it is one of the research focuses on digital currency systems.

## REFERENCES

[1] R. Courtland, "Virtual currency gets real," *IEEE Spectr.*, vol. 49, no. 6, pp. 52–53, Jun. 2012.
[2] M. L. Bech and R. Garratt, "Central bank cryptocurrencies," *BIS Quart. Rev.*, pp. 55–70, Sep. 2017. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3041906
[3] L. Sun, "Central bank digital currencies," *J. Digit. Banking*, vol. 4, no. 1, pp. 85–94, 2019.
[4] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Oct. 9, 2019. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[5] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.
[6] F. Schuh, and D. Larimer. *Bitshares 2.0: General Overview*. Accessed: Oct. 15, 2019. [Online]. Available: http://docs.bitshares.org/downloads/bitshares-general.pdf
[7] M. A. Javarone and C. S. Wright, "From Bitcoin to Bitcoin cash: A network analysis," in *Proc. 1st Workshop Cryptocurrencies Blockchains Distrib. Syst.*, 2018, pp. 77–81.
[8] E. Duffield and D. Diaz. *Dash: A Privacy-Centric Crypto-Currency*. Accessed: Feb. 30, 2019. [Online]. Available: https://cryptorum.com/resources/dash-whitepaper-privacycentric-cryptocurrency.10/
[9] Q. Yao, "A systematic framework to understand central bank digital currency," *Sci. China Inf. Sci.*, vol. 61, no. 3, Mar. 2018, Art. no. 033101.
[10] D. G. Birch, "The war over virtual money is real," *J. Payments Strategy Syst.*, vol. 13, no. 4, pp. 300–309, 2020.
[11] E. V. Sinelnikova-Muryleva, "Central bank digital currencies: Potential risks and benefits," *Voprosy Ekonomiki*, no. 4, pp. 147–159, Apr. 2020.
[12] A. Tapscott and D. Tapscott, "How blockchain is changing finance," *Harvard Bus. Rev.*, vol. 1, no. 9, pp. 2–5, 2017.
[13] G. Danezis and S. Meiklejohn, "Centrally banked cryptocurrencies," 2015, *arXiv:1505.06895*. [Online]. Available: http://arxiv.org/abs/1505.06895
[14] J. Chapman, R. Garratt, S. Hendry, A. McCormack, and W. McMahon, "Project Jasper: Are distributed wholesale payment systems feasible yet," *Financial Syst.*, vol. 59, pp. 59–68, Jun. 2017.
[15] D. Dalal, S. Yong, and A. Lewis, *The Future is Here-Project Ubin: SGD on Distributed Ledger*. Singapore: Monetary Authority Singapore Deloitte, 2017.
[16] European Central Bank, Bank of Japan. *Securities Settlement Systems: Delivery-Versus-Payment in a Distributed Ledger Environment*. Accessed: Jan. 15, 2019. [Online]. Available: https://www.ecb.europa.eu/pub/pdf/other/stella_project_report_march_2018.pdf
[17] W.-T. Tsai, Z. Zhao, C. Zhang, L. Yu, and E. Deng, "A multi-chain model for CBDC," in *Proc. 5th Int. Conf. Dependable Syst. Appl. (DSA)*, Sep. 2018, pp. 25–34.
[18] Y. Qian, "Experimental study on prototype system of central bank digital currency," (in Chinese), *J. Softw.*, vol. 29, no. 9, pp. 2716–2732, 2018.

[19] Bank of Canada Banque Du Canada, Monetary Authority of Singapore. *Jasper-Ubin Design Paper*. Accessed: Feb. 21, 2019. [Online]. Available: https://www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf
[20] J. Taskinsoy. (Jul. 20, 2019). *Facebook's Project Libra: Will Libra Sputter Out or Spur Central Banks to Introduce Their Own Unique Cryptocurrency Projects?* [Online]. Available: https://ssrn.com/abstract=3423453
[21] Y. Cao, J. Zhang, X. Yuan, T. Guo, C. Lu, G. Chen, J. Kang, X. Yan, X. Zhang, and Y. Huang, "A hybrid blockchain system based on parallel distributed architecture for central bank digital currency," in *Proc. FSDM*, 2019, pp. 1138–1145.
[22] C. Pérez-Sola, S. Delgado-Segura, G. Navarro-Arribas, and J. Herrera-Joancomartí, "Another coin bites the dust: An analysis of dust in UTXO-based cryptocurrencies," *Roy. Soc. Open Sci.*, vol. 6, no. 1, Jan. 2019, Art. no. 180817.
[23] Y. Kaneko, S. Osada, S. Azuchi, H. Okada, and S. Yamasaki, "A management method of interest-rate in UTXO model," in *Proc. IEEE Social Implications Technol. (SIT) Inf. Manage. (SITIM)*, Nov. 2019, pp. 1–6.
[24] D. Ding, K. Li, L. Jia, Z. Li, J. Li, and Y. Sun, "Privacy protection for blockchains with account and multi-asset model," *China Commun.*, vol. 16, no. 6, pp. 69–79, Jun. 2019.
[25] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.
[26] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, and S. Muralidharan, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, Apr. 2018, pp. 1–15.
[27] S. Mukhopadhyay, "Identification of normal modes responsible for ferroelectric properties in organic ferroelectric CBDC," *J. Phys. Commun.*, vol. 3, no. 11, Nov. 2019, Art. no. 113001.
[28] The People's Bank Of China. *Overall Situation of the Payment System Operation in the Second Quarter of 2019*. Accessed: Oct. 28, 2019. [Online]. Available: http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3878784/2019082217263990512.pdf
[29] H. Sukhwani, J. M. Martinez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)," in *Proc. IEEE 36th Symp. Reliable Distrib. Syst. (SRDS)*, Hong Kong, Sep. 2017, pp. 253–255.
[30] E. Anceaume, A. Guellier, and R. Ludinard, "UTXOs as a proof of membership for byzantine agreement based cryptocurrencies," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1463–1468.
[31] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.

**JINNAN ZHANG** was born in Hebei, China, in November 1982. He received the Ph.D. degree in electro-magnetic and microwave technology from the Beijing University of Posts and Telecommunications (BUPT). He is currently an Associate Professor with the State Key Laboratory of Information Photonics and Optical Communications (IPOC), BUPT, for intelligent sensing. His research interests include blockchain, AIoT, wireless communication systems, and access networks.

**RUI TIAN** received the B.S. degree in computer science and technology from Jilin University, Changchun, China. He is currently pursuing the master's degree with the Institute of Information and Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include performance analysis of blockchain systems and machine learning.

**YANGHUA CAO** received the B.Eng. degree from the Information and Communication College, Beijing University of Posts and Telecommunications (BUPT), Beijing, China, where he is currently pursuing the master's degree with the Institute of Information and Photonics and Optical Communications. His research interest includes performance evaluation for system and networks.

**XUEGUANG YUAN** received the Ph.D. degree in electronic science and technology from the Beijing University of Posts and Telecommunications, in 2009. From 2009 to 2011, he worked as a Postdoctoral Researcher with the State Key Laboratory of Information Photonics and Optical Communication, where he is currently a Lecturer. He is also a Master Supervisor with the School of Optoelectronic Information. He has published scores of papers in international academic journals and conferences and been awarded various national invention patents. His research interests include III-V semiconductor nanowires, related optoelectronic devices, and photoelectric sensing.

**ZEFENG YU** received the B.Eng. degree from the Information and Communication College, Beijing University of Posts and Telecommunications, Beijing, China, where he is currently pursuing the master's degree with the Institute of Information and Photonics and Optical Communications. His research interests include the IoT and sensing equipment.

**XIN YAN** received the B.S. degree from the China University of Mining and Technology, Xuzhou, China, in 2009, and the Ph.D. degree in electronic science and technology from the Beijing University of Posts and Telecommunications, Beijing, China, in 2014. From 2014 to 2017, he was a Lecturer with the State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, where he has been an Associate Professor, since 2018. He is the author of two books and more than 100 articles. His research interests include low-dimensional semiconductor materials and novel information devices.

**XIA ZHANG** received the Ph.D. degree in electronic science and technology from the Beijing University of Posts and Telecommunications, in 2003. In 2008, she was selected into the New Century Excellent Talents Program, Ministry of Education. She is currently a Doctoral Supervisor and a Professor with the School of Optoelectronic Information. She has published more than 100 articles in international academic journals, such as *Nano Letters*, *Nanoscale*, and *Applied Physics Letters*. Her research interests include III-V semiconductor nanowires, related optoelectronic devices, and microstructure fibers.