Journal of Computers Vol. 32 No. 5, 2021, pp. 244-256
doi:10.53106/199115992021103205021

The Design of Case-involved Property Transfer System Based on Blockchain

Cai Gong[1*], Yimin Yang[1], Zhaochong Wang[1], Yansong Zhang[2]

[1] CASIC Intelligence Industry Development Co., Ltd,
caigong@aiidc.com.cn, yangyimin@aiidc.com.cn, wangzhaochong@aiidc.com.cn

[2]Beijing Key Laboratory of Communication and Systems, School of Electronic and Information Engineering, Beijing Jiaotong University, Haidian District, Beijing, China
20120169@bjtu.edu.cn

Received 1 August 2021; Revised 1 September 2021; Accepted 8 October 2021

Abstract. In recent years, with the continuous maturity of blockchain technology, more and more applications based on blockchain appear in our life. The safe sharing and rapid disposal of case-involved property information is the focus of online case management. At present, due to some characteristics of case-involved properties, the case platform with centralized management has some issues, such as low collaborative efficiency and low intelligence. In this paper, we propose the architecture and implementation scheme of the cross departmental case-involved property transfer system based on blockchain. By introducing the blockchain technology, we have established a multi departmental case-involved property information transfer alliance chain across the public security, procuratorial and judicial departments. The case-involved property transfer system uses smart contract to implement a set of case-involved property transfer procedures designed by our investigation and research. It proposes an infrastructure of alliance blockchain based on multi-chain technology according to the business logic and makes the public security, procuratorial and judicial departments as the alliance blockchain nodes. Blockchain technology can make all nodes store transaction data. So it can efficiently realize the sharing of case-involved property information, leave traces in transaction processing and trace the processing source of case-involved properties.

Keywords: permissioned blockchain, case-involved property, information sharing, judicial, information transfer system

1 Introduction

In the judicial field, the public security, procuratorial and judicial departments have their own business systems. However, when a case occurs, these departments need to handle the case together. In recent years, more and more judicial practitioners face a large increase in various contradictions and disputes in judicial practice. In the field of judicial trial, there are many cases with few people and the channel of case information sharing is unblocked. Therefore, the public security, procuratorial and judicial departments are faced with practical problems such as how to save judicial resources and how to effectively improve the efficiency of handling cases. By establishing a case information sharing management system between the public security, procuratorial and judicial departments, the quality and efficiency of handling cases will be greatly improved. The security sharing and rapid disposal of the case-involved property information are the focus of the online case management platform. At present, there are some problems in the research and development of cross departmental case-involved property information sharing, such as segmentation, imperfect standards, low coordination efficiency and low degree of intelligence. The existing management platform adopts a centralized management mode, and the case-involved property information is uniformly managed by the central server. The centralized

* Corresponding Author

management has major security problems such as privacy disclosure. In addition, the centralized management mode has poor compatibility and scalability for the multi department collaborative case handling mechanism.

In terms of property involved in the case, when the procuratorate and the court handed over the case, due to institutional and technical obstacles, collaborative information management and property disposal have not yet been realized. As there are many kinds of property involved in the case, and the disposal methods of the property involved in different types of cases are also inconsistent, it will bring great difficulties to the management of the property involved in the case. therefore, it is of great significance to develop a system for the sharing of property information.

In recent years, with the rise of Bitcoin [1], blockchain has been extracted from Bitcoin and gradually evolved into a new technology. Blockchain has the characteristics of natural high reliability and decentralization and uses cryptographic algorithms to ensure the integrity and security of data. Blockchain has the characteristics of decentralization, and the data of the transaction process is stored in all distributed nodes. Therefore, it is very suitable for case-involved property information sharing scenarios with high security performance, data sharing, secure data storage and traceability requirements.

In view of the above problems, we design and implement a case-involved property transfer system based on blockchain, which has high security and traceability, and can make use of the characteristics of blockchain so that the sharing of case-involved property can be completed efficiently. The major contributions made in this paper are as follows: (1) It makes the public security, procuratorial and judicial departments as the alliance blockchain nodes, introducing the technology of blockchain to solve the problem of property sharing involved in the case. And we designed and implemented the architecture of the blockchain system. (2) Through investigation and research, we summarize and research the business logic of the transfer of property information among the three organizations, namely, ministry of public security, procuratorate and court, and put forward a set of business process for the transfer of case-involved properties. (3) According to the business logic, an infrastructure of alliance blockchain based on multi-chain technology is proposed, which is closely combined with the multi-organization nodes of business logic. It can provide high security and efficient business processing.

Section 2 introduces the existing research on blockchain system. Section 3 analyzes the requirements and shows the functions that the system should realize. Section 4 describes the architecture of the blockchain system in detail. Section 5 introduces two key technologies in the process of system design and implementation. Section 6 concludes the paper.

2 Related Work

Blockchain uses cryptography mechanism to ensure the security and integrity of data, which is essentially a way of distributed storage and has the characteristics of decentralization, high security, leaving traces in operation, data sharing and so on. In blockchain, the core components include consensus protocol, intelligent contract, encryption module, communication module, storage module and so on. Consensus protocol is the core technology of the blockchain. It is the rule of block generation and data writing, and the consensus protocol ensures the security and effectiveness of the blockchain. Intelligent contract is an important component of the application at the bottom of the blockchain. It is an electronic contract, which is triggered automatically when no manual intervention is allowed. Encryption module is used to provide the cryptographic basis for the blockchain providing some basic encryption and decryption algorithms and methods to construct the blockchain. Communication module is used to provide the basic unit of data exchange for the blockchain, such as the function of data propagation protocol, etc. Storage module is used to construct the storage structure of the blockchain, including the storage of the transaction, the storage of the block and so on.

At present, blockchain has mature applications in government affairs, people's livelihood, finance and other fields, because it can save every transaction information in the business process, and has the characteristics of decentralization. So it is very suitable for scenarios with data sharing, data traceability and distributed requirements. For example, Tsung-Ting Kuo et al. [2] introduced blockchain technology into biomedical and health care domains. Hu [3] applied blockchain to the tax sharing field to build a tax sharing service center etc.

The scene of cross-departmental information sharing and collaborative disposal of the property involved in the case has the characteristics of multi-organization, multi-department, complex business

process and high demand for data sharing, so the blockchain is introduced to solve the problems existing in the current transfer of property involved in the case. With effectiveness and high reliability, the system is transformed from a centralized architecture to a distributed architecture to ensure that every participating node can save transaction data. It can greatly reduce the cost of property data query, in addition, using the intelligent saving of blockchain can realize the complex business logic of property information transfer, which ensures that the business process can be strictly executed and has high security.

According to the participation mode of nodes, blockchain can be divided into public chain, federation chain and private chain [4]. Public chain is a fully public blockchain in which any node is free to join and exit. The federation chain is a polycentric or partially decentralized blockchain. Nodes need strict identity authentication to join the alliance blockchain to become alliance nodes. In the alliance chain, only the alliance node can access the data in the account book. Compared with the public chain, the alliance chain is suitable for a specific business scenario. Private chain means that all write permissions of the blockchain are concentrated in one organization, and its openness is lower than that of the alliance chain, which is usually used in scenarios such as a single enterprise. According to the business logic of the inter-departmental property transfer system, there are three organizations, namely, ministry of public security, procuratorate, and court. The system should use the blockchain structure endorsed by the three organizations. At the same time, because of the privacy of the case-involved property data, strict authentication is required for the entry and exit of nodes within the organization. Select the alliance blockchain to solve the problem of inter-departmental transfer of property involved in the case and design the transfer system of the property involved in the case.

3 System Functions

In view of the challenges faced in the actual scene, the case-involved property transfer system based on blockchain should be able to meet the full business process of inter-departmental transfer of property information, achieve efficient online processing of property involved in the case, and provide online and offline coordinated and unified alliance blockchain.

The property transfer system based on blockchain should have the following specific functions.

3.1 Processing and Conversion of Input Information of Case-involved Properties

The property involved in the case has very complex information that can be expressed by a relational structure. After the case-involved property information is entered into the system, the input obtained by the system is a kind of tree data structure, multi-dimensional information, such as Fig. 1. This kind of information can not be directly received and processed by the blockchain. Therefore, the system needs to have the function of processing and transforming the property information involved in the case, and convert the tree structure data into data that can be identified by the blockchain.

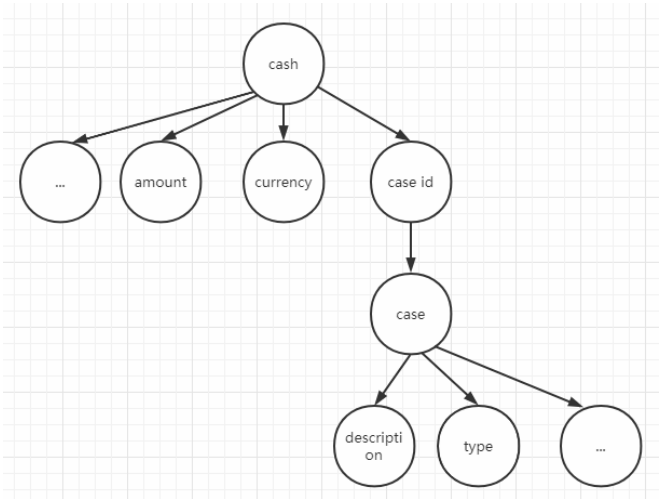

Fig. 1. An example of information structure of case-involved property

3.2 The Storage of Case-involved Property Information in the System

The case-involved property information in the input system needs to be stored in the system for subsequent transfer and query. The data of the case-involved property information is huge and the structure is complex. Therefore, the system needs to have a good storage design in order to ensure the effectiveness of the transfer of the case-involved property information in the blockchain.

3.3 The Transfer of Case-involved Property Information in the System

The transfer of the case-involved property information is the core function of the system. In the transfer function of the system, it is necessary to ensure the effectiveness and security of the transfer of the property information involved in the case. In the process of the transfer of the case-involved property information, it should be ensured that only the relevant departments have the authority to deal with the properties, and use the blockchain intelligent contract to realize the business logic of the transfer of the property information involved in the case and ensure the effectiveness. Through the blockchain block storage to achieve the operation of the transfer of case-involved properties to leave a mark to ensure security.

3.4 Management of Federated Users and Nodes

As the transfer of the case-involved property information takes place in a specific organization and between specific departments, the system should adopt the structure of alliance chain. After the system is started, the participating nodes in the system and the department users involved need to be managed, and the nodes and users involved need to be authenticated.

3.5 Coordination and Unification of Online and Offline

Because the blockchain can not be tampered with, the transfer system of property involved in the case based on the blockchain should be able to ensure the coordination and unity of online and offline data processing. The business process of online property information transfer must be consistent with the actual business offline, at the same time, it needs to be combined with the user rights management function to achieve the effectiveness of online and offline data processing.

3.6 Blockchain Related Functions

The bottom layer of the property transfer system based on blockchain uses blockchain as the core data processing component, which can provide efficient and secure storage and transfer of property information data through blockchain. Therefore, the system needs to be able to provide some blockchain-related functions, such as blockchain index, blockchain visualization and so on.

4 System Architecture

The transfer system of the case-involved property on the blockchain should be able to achieve efficient online processing of the property involved in the case under the required business logic requirements, and can provide a unified online and offline processing process. The system architecture model is shown in the Fig. 2. Each node of the alliance chain usually corresponds to the organization of an entity, and the joining and withdrawal of the node need to be authorized. The ministry of public security, the procuratorate, the court and other agencies form case-related alliances to jointly maintain the normal operation of the blockchain network. The nodes added to the blockchain can set up their own database to store the local blockchain information, and transmit the transaction information and blockchain through P2P network broadcast. According to the function of the system described in the previous section, the architecture of the property transfer system is designed, and a five-layers architecture model is proposed shown in Fig. 3, which is constructed by alliance chain, and there is no currency transaction compared with the public chain. So the incentive layer is reduced.

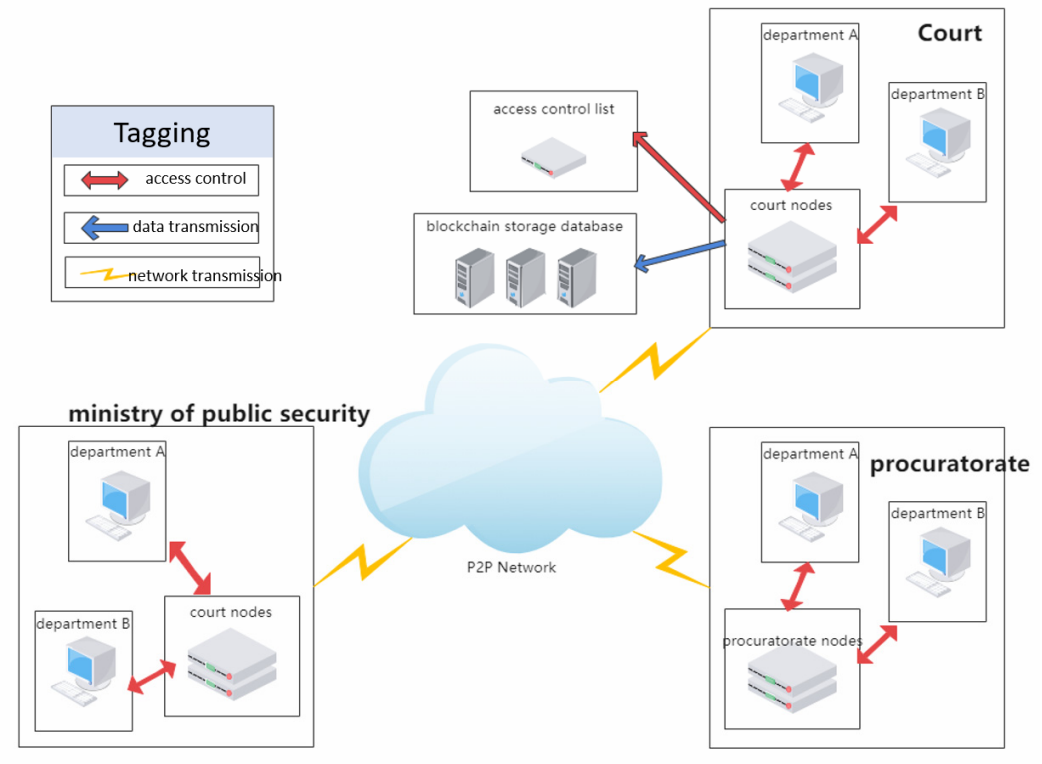

Fig. 2. The architecture model of case-involved property transfer system

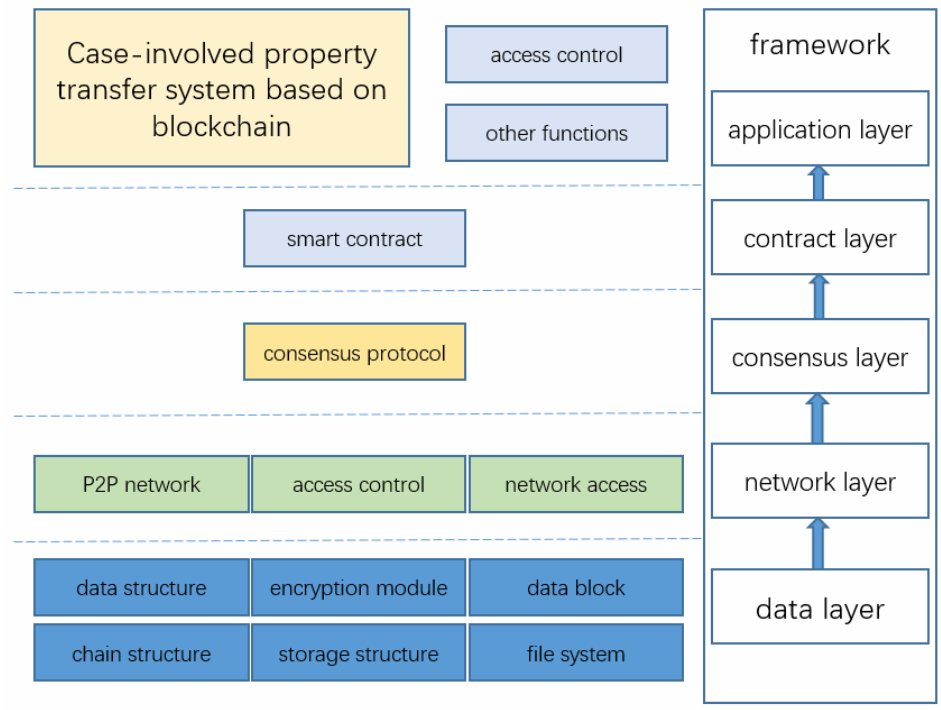

Fig. 3. Five-layers architecture model

4.1 Case-involved Property Information Processing and Storage Module

The details of the case-involved property need to be processed and converted when they are entered into the blockchain system. In order to ensure the efficient operation of the underlying blockchain network, in the cross-department transfer system of the blockchain, the underlying blockchain network flows the

identification number that can uniquely represent the current case-involved property, while the details of the case-involved property can be converted into tables and stored in the relational database.

A string with a length of 8 is used to represent the unique identification number of the property involved, which occupies 8 bytes, as shown in the Fig. 4. The first two bits of the string represent the types of property involved, of which the first bit is 0 for movable property, 1 for real estate, 2 for bonds, for example, 00 for cash, 01 for deposit, 02 for electric motor, 03 for vehicle, 10 for land, the middle two digits of the string represent the year of the property involved, 19 represents the case in 2019, 20 indicates the case in 2020, and the last four digits in the string represent the serial number of each type of property. The unique identification number of the property involved in the case stored in string format can achieve two basic functions: one is to uniquely represent the case-involved property information, and the other is to run and save in the blockchain, which can realize the fast and efficient operation of the underlying blockchain network.

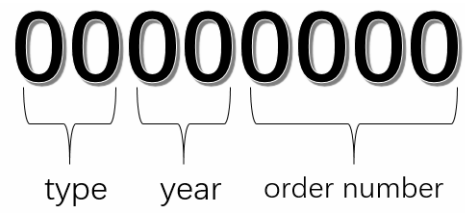

Fig. 4. Unique identification number of case-involved property

The details of the property involved will be stored in the relational database, and the Table. 1 shows the detailed characterization structure of several kinds of property extracted from the original case file through research. The structure of the property information involved in the actual scene is complex, but we conclude that it can be expressed by tree data structure. In relational database, a data structure can be transformed into multiple associated tables for storage.

Table 1. Structure of several kinds of properties

vehicle	cash	deposit	land	motor
License plate number	Currency	Bank of deposit	Valid address	Name
Car name	Amount of money	Account number	Unit of measure	Specification / model
Registration Certification No	Processing flow	Currency	Quantity	Unit
Original registration date	Case description	Book value	Purchase value	Quantity
Remark information	Unique identification number	Adjust debit	Evaluation value	Appraisal value
Processing flow		Adjust credit	Evaluation organization	Remark information
Case description		Adjust book value	Evaluation date	Processing flow
Unique identification number		Remark information	Discount rate	Case description
		Processing flow	Certificate No	Unique identification number
		Case description	Policy No	
		Unique identification number	Insurance period	
			Lease status	
			Rent standard	
			lessee	
			Possession status	
			Processing flow	
			Case description	
			Unique identification number	

In addition to the storage of the property involved in the case, the storage module also provides the blockchain data storage function, including the block data of the blockchain and the state data of the blockchain. The block data of the blockchain stores every transaction information in the blockchain network, which is the transaction log. It records all the changes that contribute to the current state, and the transaction is stored in the block and is linked to the blockchain. The block data in the blockchain cannot be tampered with. The block data should be stored in the local hard disk of all distributed nodes in the alliance chain in the form of binary files. when the alliance chain has multiple blockchains, the distributed node will save multiple binary block data files.

The block includes three parts: the block head, the block data and the block metadata, where in the block head contains three fields, which are the block number, the hash value of the previous block head and the hash value of the current block. The block head is written when the block is created. The block data contains an ordered list of transactions, which together make up the "transaction log". The block metadata includes the time when the block was written, the certificate, public key and signature of the block writer, and some configuration data of the consensus mechanism.

Because the block head of a block contains the hash value of the previous block head, all blocks are closely linked and can not be tampered with, forming a blockchain.

The state data of the blockchain is designed as a database to store the latest status of each account. Through the state database, you can directly access the latest value of an account state, and you do not need to traverse the whole blockchain block data to calculate the current value.

The storage of state is realized in the form of database, which aims to provide simple and effective state storage and retrieval of account books. The state database is constructed by CouchDB. When the account status structure is an JSON document, CouchDB can support various forms of query and update of these data. CouchDB runs in a separate operating system process and can be installed locally or set up on a server external to the system.

4.2 Consensus Module

In the distributed system, the consensus algorithm needs to be used to ensure the consistency of the data records of each node in the network. The consensus mechanism is the rule of block generation and data writing. Through the data consensus between nodes, transaction data can be prevented from being tampered with, and the consensus algorithm can also undertake the function of transaction validity verification. Consensus module is the core technology of blockchain, which will affect the security and reliability of the whole system.

Consensus algorithms can be divided into two types [5]: consensus algorithms based on proof mechanism, such as PoW, PoS [1, 6], etc., and consensus algorithms based on voting, such as Raft, PABT [7-8], etc. Among them, the consensus algorithm based on proof mechanism is usually used in the common chain, which can provide high security, but its efficiency is usually low. In the business logic of property information transfer in the case, the system usually requires a high consensus efficiency. For example, the system can provide at least the transaction processing capability of 1000TPS, and the system will use alliance chain for architecture. Each participating distributed node is constrained by the identity authentication module, and the system's requirements for the security performance of the consensus algorithm are relatively small. Therefore, the consensus module should adopt the consensus algorithm based on voting, which is more efficient and meets the business requirements of property transfer involved in the case.

Consensus algorithms based on voting can also be divided into two types: one is an algorithm that can tolerate Byzantine errors, such as PBFT, the other is an algorithm that can only tolerate crashing nodes, but cannot allow evil nodes to exist, such as Raft. In the property information transfer system across three organizations, namely, ministry of public security, procuratorate, and court, all nodes run in an internal network environment, that is, a credible and controllable operating network. In this environment, the probability of the existence of evil nodes and the difficulty of doing evil will be greatly increased, and we can focus on the improvement of operational efficiency. Therefore, the consensus algorithm of Raft type is used in the consensus module of the property transfer system involved in the case, so as to ensure that the system can have higher operating efficiency.

4.3 Business Module

Intelligent contract is a key technology to connect the underlying blockchain network with top-level users. Application layer users can use certain protocols, such as RPC, through reserved interfaces, such as RPC service interface, to communicate with intelligent savings. Therefore, intelligent saving is time-driven, stateful, multi-party recognized and running on blockchain programs. Its biggest advantage is to use program algorithms instead of artificial arbitration.

In the transfer system of case-involved property based on blockchain, the business logic of property information transfer is realized through intelligent contract, and the intelligent contract which is trusted by distributed nodes and whose content is completely consistent is used to ensure the validity, security and integrity of the business logic of property transfer involved in the case. The transfer of case-involved properties across public security bureaus, procuratorates and courts is usually complex, which involves the transfer of cases between nodes of multiple organizations and departments. Therefore, intelligent saving is written through Turing's complete computer language, so that more complex business logic can be realized.

The intelligent contract should be installed and run in an environment independent of the distributed node process, such as the Docker environment. After the installation of the intelligent contract is completed, it should be able to realize the self-start of the contract, that is, when the distributed node receives the transaction message, it can automatically start the intelligent contract in the Docker environment and call the contract code to execute the transaction message through intelligent and economical writing and deployment. The complex business logic of property transfer can be reproduced in a safe and efficient way.

4.4 Identity Module

As the blockchain property transfer system is constructed in the way of alliance chain, the system needs to have a strict identity authentication module to verify the identity of each distributed node that participates in the consensus. At the same time, because the property transfer business involved in the case has the characteristics of multiple identities and multi-users, and the scope of the transfer business is the ministry of public security, the procuratorate and the court, the identity and authority of each node must be clear. The input of the node is added manually by the upper-level administrator, and the joining and leaving of the node need to be authenticated by all distributed nodes.

Because the consensus module uses the Raft consensus mechanism, the identity module is the key to ensure the normal operation of the consensus module. It needs to be able to effectively avoid evil nodes to join, nodes to join the internal network environment need to go through the first layer of identity authentication, in the internal network environment to join the blockchain network needs to go through the second layer of identity authentication, through the dual identity guarantee mechanism to achieve high security and high reliability of the alliance chain. At the same time, due to the small number of distributed nodes needed in the property transfer system, the identity key generation and distribution of each node are realized manually to further improve the security performance of the system.

4.5 Network Module

The network module is the basis for the normal operation and use of other modules, and it needs to achieve three functions: the first is to realize the data exchange and consensus among the distributed nodes of the blockchain network; the second is to realize the data exchange between the system application layer and the blockchain network; the third is to realize the data access between the client (front end) and the system server (back end).

Blockchain network mainly relies on Gossip protocol to transmit data, and provides gRPC interface to the outside to access and request important functions. The underlying layer of the cross-departmental property information handover system based on blockchain is a decentralized Internet system that relies on nodes to exchange information. Data is distributed through Gossip protocol. Because the service is scattered among nodes, local nodes or networks are destroyed with little impact on the rest, so it has the advantages of anti-attack and high fault tolerance.

The network module at the bottom of the system also provides the communication function of gRPC service, and the idea of RPC is very common in the blockchain. Through the remote procedure call, the

client can access some functions provided by the underlying blockchain system, thus realizing the business logic of the transfer of property information involved in the case. For example, the intelligent contract call in the blockchain network, the upper application submitting the transaction message to the blockchain network, and the data exchange of the consensus process between the blockchain nodes can all be realized through gRPC.

The data interaction between the system application layer and the blockchain network mainly includes: the application layer calls the intelligent contract provided by the blockchain to realize the property transfer business logic involved in the case, and the application layer calls the blockchain consensus interface to realize the sharing of transaction messages. The two scenarios of data interaction can be completed by setting gRPC services in the blockchain system.

The access between the client and the system server can be completed by the traditional communication between the front-end and the back-end server. The system can provide some Restful interfaces for the front-end calls in the back-end, and realize the data exchange through Http protocol. At the same time, the identity authentication module is used to authenticate the front-end users to achieve the effectiveness and security of the transfer of property information involved in the case.

5 Key Technologies

5.1 The Business Logic of Property Information Transfer across Public Security Bureau, Procuratorate and Court

The transfer process of property information across public security bureaus, procuratorates and courts is related to the types of cases. Because there are many kinds of case-involved properties, the data structure is complex, and the transfer process of property involved in the case also has certain local characteristics, it can not be completely unified, so through investigation and research, we summed up a process of property information transfer among public security bureaus, procuratorates and courts. The process fully covers all the case-handling departments of the ministry of public security, the procuratorate and the court, and it is a detailed and referable business logic for the transfer of information of the property involved in the case across the public scurity bureau, the procuratorate and the court. The specific business process is as follows.

The specific public security departments conduct the entry, review and storage of the original cases. Ordinary police officers enter the original case information, which is reviewed by the leaders of their units, and then the internal police officers of their units perform storage registration.

Moving the case-involved properties to the warehouse of evidence center. When the case needs to be transferred to the procuratorate, the personnel of the police station who is involved in the case need to transfer the items of the case to the evidence center for unified management before the transfer to the procuratorate. The specific process is as follows. The police from police station apply for the transfer of the treasury, and the leader conducts the review of the application. Then the internal policemen move the involved case out of the warehouse, and finally, the evidence center personnel will receive the material evidence.

Transferring to procuratorate and court. After the evidence center receives the material evidence, the personnel of the police station carry out the transfer to procuratorate and court. The specific process is as follows: the police from police station applies for the transfer, and the leader conducts the transfer review. After the review is passed, the legal brigade will review it and the final data will be automatically pushed to the clerk of the procuratorate.

Acceptance and processing by the procuratorate. The procuratorate clerk will receive the case information transferred by the public security departments. The procuratorate clerk can view the received case. Once the case is received successfully, the right to handle the case will automatically be transferred to the procuratorate, and the original unit will no longer be able to handle the case accordingly. The procuratorate could apply to second for confirming the material evidence information. The process is as follows: the procuratorate clerk makes a secondment application, the procuratorate leaders review, the management personnel of the evidence center perform the secondment out of the warehouse, hand over the borrowed items to the procuratorate, and then perform the secondment return operation when it is returned by the procuratorate.

Acceptance and processing by the court. After the procuratorate determines that the case meets the requirements for prosecution, the case information will be transferred to the court. The process is as follows: the procuratorate clerk initiates an application and the procuratorate leader reviews it. Then the case data will be automatically pushed to the court clerk, and a dedicated person will perform classified management. After the court clerk receives the case, he will carry out operations such as leaving, destroying, confiscating, and entering the state treasury. The specific procedures are as follows:

Ex-warehouse: The court clerk makes an application for ex-warehouse, then the leader reviews, and the evidence center carries out ex-warehouse registration based on the court's judgment and relevant documents.

Destruction: The court clerk makes an application for destruction, the leader reviews it, and the evidence center conducts the destruction registration based on the court's judgment and related documents;

Confiscation: The court clerk makes an application for confiscation, the leader conducts the confiscation review, and the court clerk evaluates the goods, and then the physical objects are realized and registered in the state treasury.

5.2 The Infrastructure of Alliance Blockchain

According to the business logic of the inter-departmental property information sharing system, the relevant different types of business can be summarized. It includes the transfer business of the case-involved properties among the public security bureau, the procuratorate and the court organizations, the transfer business of the storage location of the case-involved property with the material evidence center as the core, and the business within some organizations, such as the input business of property involved in the case between public security departments and so on. According to different business types, different alliance blockchains can be created, with a total of five blockchains in parallel. Multiple chains are used to realize the complex collaborative disposal of property involved in the case. The blockchain data are independent of each other, and the processing efficiency is higher and the security is better.

The schematic diagram of the logical structure of the blockchain is shown in the Fig. 5, Fig. 6 and Fig. 7.

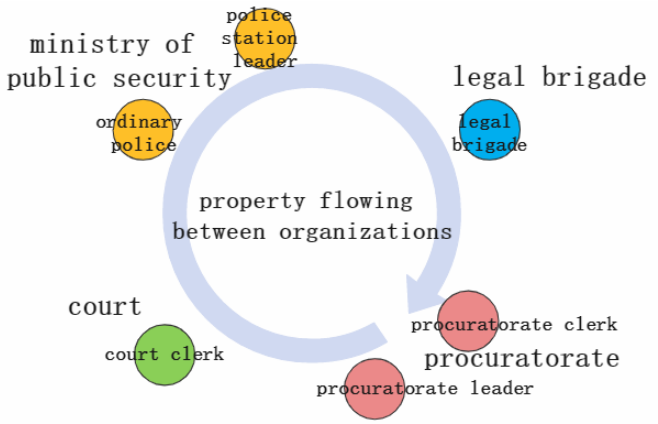

Fig. 5. The blockchain of case-involved property transferring between three organizations

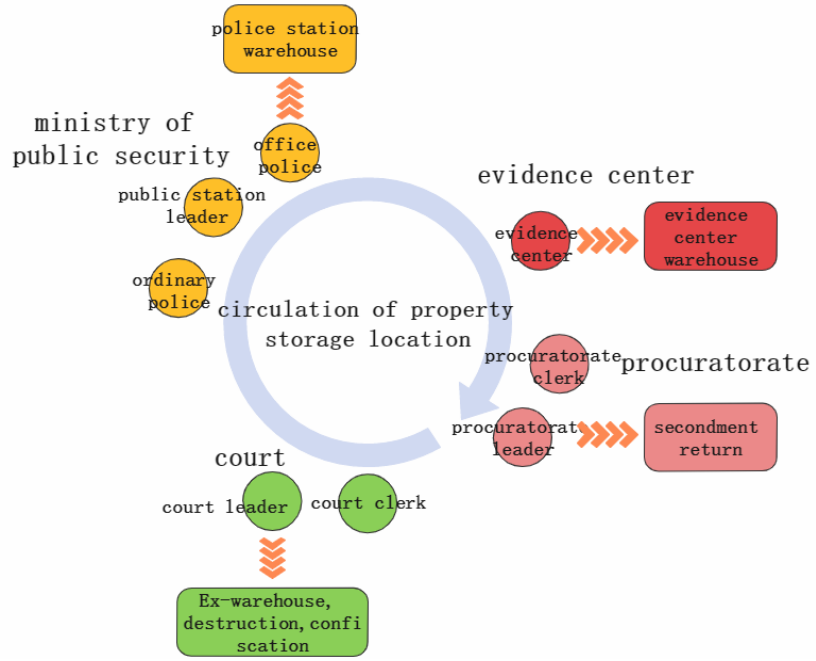

Fig. 6. The blockchain for storage location circulation of case-involved property

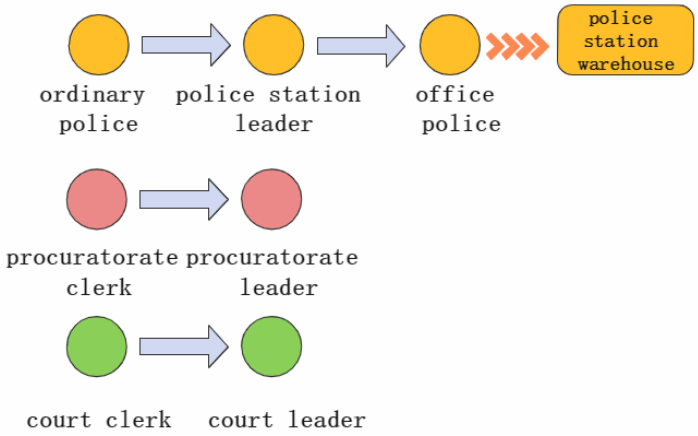

Fig. 7. Organization internal business blockchains

Fig. 5 shows that only a small number of department nodes can participate in the transfer process of property involved in the case between organizations. In this blockchain, the information flow takes the place of ownership of the property involved as the core, which is the basis of other blockchains. Fig. 6 is a blockchain specially used to represent the storage location conversion of the property involved in the case. the information flow is carried out with the warehouse where the property is located as the core, and the nodes that maintain the blockchain can view the current warehouse location of the property involved in real time. Fig. 7 shows three business blockchains within the organization, which are only responsible for the business logic within the organization. The first participating node is only the node within the public security department, which is used to provide the input function of the property involved in the case within the public security department. The second is the blockchain within the procuratorate, which is used to provide functions such as secondment and return between the procuratorate departments, and the third is the blockchain within the court. It is used to provide the function of adjudicating the case-involved property between the departments of the court.

At present, in the process of research and development, the alliance chain data processing for a specific business mainly uses the single chain mode, which has the advantages of simple and convenient implementation. However, for the case-related property information sharing business with complex business logic, multi-organization and multi-departments, the use of single-chain mode is less secure. In

addition, the property information sharing business has the characteristics of multi-levels and clear powers and responsibilities. And parts of the business only require the participation of some nodes, not all nodes, so the use of single chain will cause a lot of redundancy.

In the parallel blockchain structure of business-oriented multi-alliance chain, the five blockchains will interact with each other, so there will be cross-chain operations, and cross-chain operations focus on two behaviors: one is the storage location of the property involved in the case changes, and the other is when the attribution of the case-involved property changes. When the storage changes, such as the case-involved property is transferred from the police station warehouse to the physical evidence center warehouse, the police of the police station need to apply first, and after the examination and approval by the leaders of the police station, the internal police will move out of the warehouse, and the application review stage takes place within the police station, so this process takes place in the business blockchain within the organization. On the other hand, the transfer operation of the internal police to the warehouse will involve the change of the location of the case-involved property, which will need to be transferred by calling the blockchain in Fig. 6, which will involve cross-chain operation. When the ownership of the property involved in the case changes, for example, in the process of transfer and inspection of the property involved, it needs to be first applied by the police of the police station, examined by the leader of the police station, and approved by the legal brigade and automatically transferred to the procuratorate, this process involves the change of the attribution place of the police station to the procuratorate, and the internal business blockchain of the organization needs to call the blockchain in Fig. 5 for circulation. Cross-chain operations are implemented based on nodes trusted by both chains and triggered by business blockchains within the organization. Through these “interactive” nodes, one blockchain can update the data of another blockchain. In Fig. 5 and Fig. 6, blockchains only passively receive cross-chain requests. In addition, there is no interaction between the three blockchains in Fig. 7. That indicates that the business logic within the organization cannot be perceived by the external organization.

The infrastructure of the case-involved property alliance blockchain is designed strictly according to the business logic. On this basis, the intelligent contract of the blockchain is designed and realized at the same time, so that the underlying blockchain system can effectively realize the transfer of case-involved properties across public security bureaus, procuratorates and courts.

6 Conclusion

Aiming at improving the efficiency of the inter-departmental co-processing of the case-involved properties and the security of the transfer system, the paper investigated a variety of existing application based on blockchain. We proposed the architecture and implementation plan of cross-departmental case-involved property transfer system based on blockchain. It uses smart contracts to implement the business logic of transferring case-involved property between multiple departments of the three organizations of public security, prosecution and court. By introducing the blockchain, each node in the transfer system can store the transaction data of the case-involved properties. By using a decentralized architecture can improve the security of the transfer system and can make the system an alliance jointly maintained by ministry of public security, procuratorate, and court, which is more suitable for actual business scenarios.

Acknowledgements

This work is support by National Key R&D Program of China (2018YFC0832303).

References

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>, 2008 (accessed 29.03.20).

[2] T.T. Kuo, H.E. Kim, L. Ohno-Machado, Blockchain distributed ledger technologies for biomedical and health care applications, Journal of the American Medical Informatics Association 24(6)(2017) 1211-1220.

[3] Q.L. Hu, Research on the Application of Blockchain Technology in the Field of Tax Sharing, Friends of Accounting 11(2021) 150-156.

[4] Y. Yun, S. Xu, Overview of blockchain technology, Journal of Quality and Certification 5(2020) 56-58.

[5] G.-T. Nguyen, K. Kim, A survey about consensus algorithms used in blockchain, Journal of Information Processing Systems 14(1)(2018) 101-128.

[6] S. King, S. Nadal, Ppcoin: Peer-to-peer crypto-currency with proof-of-stake, in: Proc. 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016.

[7] D. Ongaro, J. Ousterhout, In search of an understandable consensus algorithm, in: Proc. 2014 USENIX Annual Technical Conference, 2014.

[8] C. Miguel, B. Liskov, Practical byzantine fault tolerance, in: Proc. the Proceedings of the Third Symposium on Operating Systems Design and Implementation, 1999.