Blockchain Based Certificate Deposit System for Judicial Departments

Zhaoxing Jing[1,2], Chunjie Cao[1,2], Xiaoli Qin[1,2](✉), and Hao Wu[1,2]

[1] School of Cyberspace Security, Hainan University, Haikou 570228, China
Xlqin@hainanu.edu.cn

[2] Key Laboratory of Internet Information Retrieval of Hainan Province, Haikou, China

Abstract. In the traditional judicial system, the public security, procuratorate, court and judicial bureau all involve private information, so the data current and sharing of each department will be greatly restricted. To solve these problems, a blockchain-based public security, procuratorial, and judicial evidence storage system is designed, which can, to a certain extent, solve the morass of data sharing among various departments of the judicial system, and can ensure the privacy of data. The proposed scheme uses the chain structure of the permissioned chain FISCO BCOS as the blockchain platform and combines the Merkle tree and hash function to access data. The structural storage of data can ensure that the uploaded data is traceable and without being tampered with. The public security, judicial and judicial evidence storage system designed with blockchain technology can realize database sharing among various departments of public security, procuratorate, court, and judicial bureau, eliminate the risk of leakage and tampering in the process of case evidence flow, and protect citizens' privacy and national information safety.

Keywords: Certificate Deposit System · Public Security · Procuratorial and Judicial Departments · Blockchain · Merkle Tree

1 Introduction

Traditionally, in the entire judicial enforcement project, the databases among the public security, procuratorate, courts, and judicial bureaus are independent of each other. The information systems of each department are in an independent and closed state. However, case acceptance, deadline control, document delivery, and other links require the connection of various departments. Consequently, case information cannot be transmitted in real-time, and complete data cannot be provided for higher-level departments' plans, which would largely affect case handling efficiency. On the other hand, various departments of the Public Security, Procuratorate and Judicial Department use their own credit to provide services such as depository, preservation, and witnessing of electronic data. However, there are many institutions for the circulation of case evidence, and the risk of being leaked and tampered with is high. Citizen privacy, once leaked or tampered with, the consequences will be unimaginable.

J. C. Hung et al. (Eds.): IC 2023, LNEE 1045, pp. 689–697, 2023.
https://doi.org/10.1007/978-981-99-2287-1_96

The emergence of blockchain technology has provided a new solution for the handover between traditional public security, procuratorial, and judicial departments. Through blockchain technology, the public security, procuratorate, court, and judicial bureau are placed in the blockchain ecosystem, and through the multi-level authority management of smart contracts and interfaces, government affairs processing and data sharing within a certain range are realized. Blockchain is a distributed ledger whose nodes involve data encryption, timestamping and consensus mechanisms. Due to the distributed storage of data, if one node is breached, it will not affect the overall data, and it is more difficult for the whole node to be breached. Securely handle sensitive information through smart contract authorization. At the same time, the data on the blockchain is non-tamperable and traceable, which can realize the immediate handling and accountability of data leakage incidents.

This project develops the integrated blockchain certificate deposit system for public security, procuratorial and judicial departments, which further improves the transparency, credibility and public satisfaction of judicial work in the advancement of smart city construction. It will provide a model for cross-departmental business collaboration and data sharing, which is indispensable to building an efficient and intelligent Smart City.

2 Related Work

Since the concept of blockchain was proposed, its implementation in various fields has been carried out.Bonomi et al. [1] proposed an improved monitoring chain (B-CoC) developed by Ethereum to automate the process of monitoring the chain to guarantee evidence integrity and traceability to the owner in the system. Ichikawa D et al. [2] developed and evaluated a trusted, auditable and tamper-proof mobile health system based on blockchain technology using a distributed network to address the problem of data management when mobile health information data is stored in a server. Chao Xie et al. [3] proposed a dual-chain architecture and proposed a data security storage scheme that is based on the puzzle that it is difficult to automatically store information on the chain when conducting blockchain traceability of agricultural products. The agricultural product quality data tracking in the blockchain ensures that the agricultural product data is not tampered with in the system. Yuqin Xu et al. [4] designed an education system for the problem that the current digital infrastructure for managing educational certificates cannot ensure the security of data and the trust of system, and most of the current blockchains rely on tokens, which cannot accurately and efficiently support certificate queries. The certificate manages the blockchain. It only takes a short time to realize the verification of the block, and at the same time, it can provide efficient on-chain transaction queries and historical transaction queries of on-chain accounts. Rui Q et al. [5] proposed a blockchain-based secure storage scheme for dynamic data in view of the possible tampering and forgery in the secure storage of dynamic data. Analyze the consistency between the local behavior of the consensus terminal to maximize its own interests and the overall goal of ensuring the overall security and effectiveness of the system through mathematical models, and design a consensus mechanism suitable for dynamic data security storage, data ownership state transition mechanism and storage

System architecture. Cebe et al. [6] constructed a permissioned blockchain scheme to tackle post-mortem analysis of traffic accidents in the Internet of Vehicles and put various sensory data collected by vehicle sensors on the blockchain, which can use the minimum storage space and handling overhead to enable post-incident analysis with traceable, trustless, and private information. Ryu et al. [7] proposed a digital forensics framework for IoT infrastructure based on blockchain technology, aiming at the problem that the current law enforcement agencies cannot meet the heterogeneity and distribution characteristics of digital forensics tools, investigation frameworks and processes in the IoT-related issues. Thus, the robustness of the existing depository data hosting process is improved. In their paper, Saraju P [8] et al. introduced the first-ever blockchain application in the IoT field that can tackle device limitations and data issues, in order to solve the scalability and latency. The consensus algorithm of this blockchain is better than Traditional PoW is 1000 times faster. Christian [9] studied the limitations of traditional encryption and access control models to solve security and privacy issues in the trend of transferring data and services in the healthcare field to the cloud. Nurzhan [10] studied the information security and privacy issues of transaction data in the smart grid field with interactive capabilities and combined blockchain technologies to overcome the security issues related to distributed smart grid power transactions in multiple ways. Miyachi Ken [11] et al. aimed at the problem of on-chain and off-chain collaboration in blockchain, explored the interaction between on-chain and off-chain storage and computing, and applied it to the medical industry, and proposed a modular hybrid privacy protection model, applied in three different reference frames, to protect medical privacy data.

3 Methods

3.1 Permissioned and Permissionless Chains

At present, the underlying platform of blockchain can be categorized into two types, namely permissioned chain and permissionless chain. This section will compare the two types of chains from multiple perspectives and evaluate the correct chain type selection.

In 2008, a scholar under the pseudonym Satoshi Nakamoto proposed Bitcoin, a decentralized digital currency payment system that does not require the endorsement of any authority. Later, it was discovered that the basic technology blockchain in Bitcoin, can also be employed in handling trust issues in information transmission between devices without trusting each other and without third-part intermediaries. To this end, a number of blockchain platforms, represented by Ethereum, have emerged to realize digital asset transactions. Any node can join/exit at any time without permission, so this type of blockchain is called a permissionless blockchain. The feature of permissionless chain that allows any node to enter and exit at will is obviously not suitable for enterprise-level applications. In a cross-institutional transaction scenario, multiple companies that cooperate with each other form an alliance, and only members of the alliance can join the blockchain and participate in transactions. A blockchain in which such nodes require permission to join is called a permissioned blockchain. Permissioned and permissionless blockchains target different application scenarios and solve different problem areas. The main differences between them are shown in Table 1.

Table 1. Comparison of Permissioned and Permissionless Chains

	Permissionless chain	Permissioned chain
Node admission	Nodes join freely	Nodes need permission to join
User management	Any user can join, the user identity is anonymous	Users need to be verified before they can join, and the user's identity is real-name
Decentralization	Deployed on a global scale to achieve complete decentralization	Deployed in the enterprise alliance to achieve multi-centralization
Consensus mechanism	Proof-based: PoW and POS	Voting-based: PBFT and Raft
Digital currency	Issue digital currency to motivate more nodes to participate in bookkeeping and operations	Built for inter-enterprise business without issuing digital currency and incentives
Transaction storage	Each node stores the entire network transaction data in full	Due to the trade secrets involved, each node consistently stores the hash of the transaction data related to its own business and the transaction data of other parties

As can be seen from the above table, due to the openness and completely decentralized structure of the non-licensed chain in terms of node access, user management, decentralization, consensus mechanism, etc., it is not suitable for the field of public security, procuratorial and judicial departments. Therefore, this system selects the permissioned chain as the available chain type. The mainstream underlying platforms of such chains are Hyperledger Fabric of the Linux Foundation, FISCO BCOS of the "Golden Chain Alliance", Coco of Microsoft, Enterprise Ethereum Alliance (EEA) and Corda of R3.

3.2 Merkle Tree

Merkle trees are a fundamental part of the blockchain. Merkle tree, also known as hash tree, is an important technical algorithm used in blockchain data storage. After the encryption process, the information extracted from the data stored in blocks will be stored in the node of a Merkel tree as a hash value. Hash trees can be used to authenticate data stored, processed, and transmitted in and between computers without considering the format of the data. The merits of the Merkle are that it can achieve a high level of security without losing the data transferring rate between devices and suffering from loss and tampering (Fig. 1).

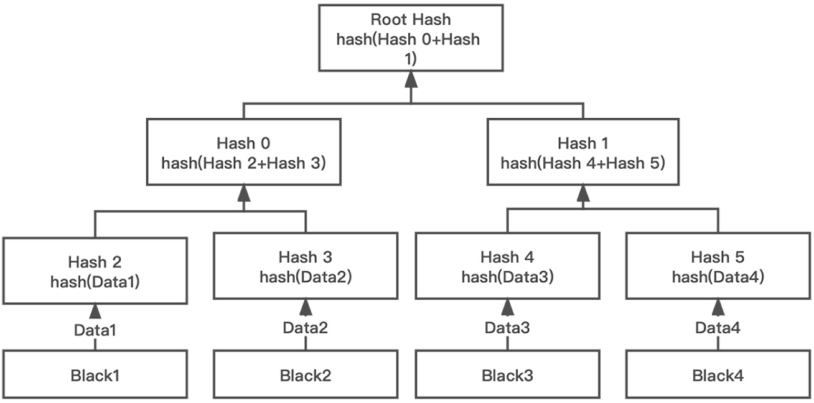

Fig. 1. Basic structure of Merkle tree

4 System

4.1 System Framework

The whole system framework design is mainly divided into four layers, namely data acquisition layer, data processing and chaining layer, data sharing layer, and application empowerment layer.

The data collection layer realizes the collection of the original data of various public security, procuratorial and judicial departments. To ensure the authenticity of the data before uploading to the blockchain, the identity of the data uploader is necessary to be identified and verified ahead, and the corresponding data to the data uploader in the organization through CA certification also need to be issued. The certificate ensures that the identity of the data uploader is authentic and credible. After identity verification, the data uploader can upload the relevant original data of the case.

The data processing and chaining layer mainly completes the following tasks: process the original case evidence, case-related documents and other information to ensure that the data to be uploaded to the chain is encrypted and protected, and after completing the encryption of the original data, receive data upload request, upload the encrypted and authoritative and reliable judicial evidence and other information to the blockchain for storage so that the uploaded data is traceable and cannot be tampered with.

The data sharing layer mainly completes the distributed sharing of judicial data privacy protection on the chain. At the same time, it cooperates with the control of regulatory power to protect the data security of all parties, and enables the relevant evidence and other data to flow in each judicial institution. Institutions and the public with supervisory authority can view the plaintext data of relevant case data and grasp the real situation.

The application empowerment layer is mainly oriented to business needs and builds a judicial evidence traceability system. All types of users can access the system after unified authentication through the user access interface. Different users set different query permissions, and users can search for relevant information through keyword searches. Case evidence is recorded on the chain (Fig. 2).

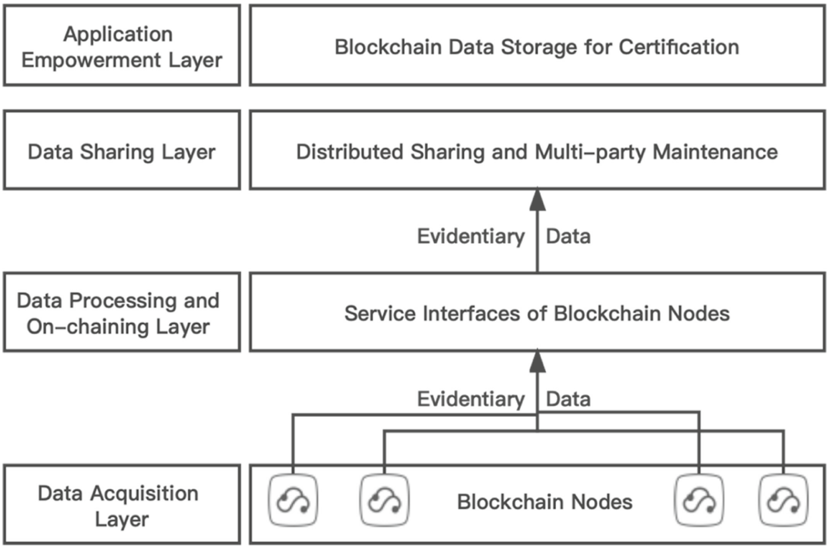
Application Empowerment Layer
Blockchain Data Storage for Certification
Data Sharing Layer
Distributed Sharing and Multi–party Maintenance
Evidentiary Data
Data Processing and On–chaining Layer
Service Interfaces of Blockchain Nodes
Evidentiary Data
Data Acquisition Layer
Blockchain Nodes

Fig. 2. Blockchain-based framework of the public security, procuratorial and judicial department certificate storage system

4.2 Block Structure

Blocks are the basic unit of a certain blockchain, normally it composes a block header and a block body. Version information is stored in the block header, such as the time when the block was generated (timestamp), the hash value of the subblock, and root node data of Markle tree which can summarize and quickly summarize all the data in the verification block. The block body uses the structure of Merkle tree to store data. Each node stores a hash value. Each leaf node at the bottom corresponds to a hash value of data information. Its parent node is two hash values again. Hash, and recursively get the final Merkle root hash (Fig. 3).

In the process of processing a case, a lot of documents and evidence will be generated. The uploader extracts keywords for the query according to the type and content of the data and generates an index from the keywords to describe the data, data abstract, data generation time and the original data is packaged into a file at the address stored in the local library. First, the abstract of the file is obtained, and the file is encrypted to generate a ciphertext. Utilizing his own private key, the uploader signs the index, file ciphertext, and file abstract and uploads it to the blockchain. After uploading all the evidence information in each link, the uploader also needs to generate a piece of information indicating the progress of the case, sign it with the private key and upload it to the blockchain. The

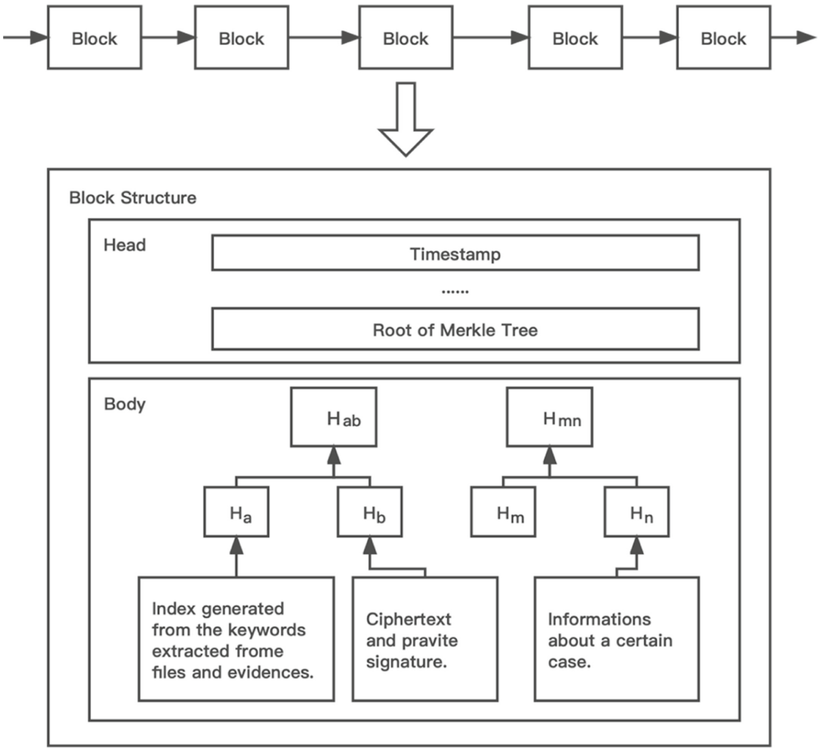
Block
Block
Block
Block
Block
Block Structure
Head
Timestamp
......
Root of Merkle Tree
Body
Hab
Hmn
Ha
Hb
Hm
Hn
Index generated from the keywords extracted frome files and evidences.
Ciphertext and pravite signature.
Informations about a certain case.

Fig. 3. Block structure

last leaf node of the Merkle tree of each block stores the information. It is the hash value of this piece of information, and the case information is stored in plaintext on the blockchain for the public query.

4.3 Performance

The emergence of electronic evidence has brought great changes to the judicial certification system. The development of electronic evidence has adapted to the tide of informatization, which is of great significance for improving judicial efficiency and reducing judicial costs; building a free trade port is a long-term and arduous task. In this process, legalization, transparency, and regulation are the objective requirements for building a high-level free trade port in the world. This system uses blockchain and other technologies to integrate and modernize the certificate deposit system and strengthen the application of the social credit system. Strengthen data security sharing and disclosure, improve government services and governance, and build a free trade port governance system with complete systems, scientific norms, and effective operation. Use zero-knowledge proof, verifiable secret sharing technology to protect data privacy and computational verifiability; use trusted input loading to ensure data authenticity. At the same time, the use of distributed ledger records ensures that the entire process service records of joint computing between entities can be verified and traceable. The improvement of the government's judicial credibility is significant to continuously promote the formation of high value-added industries in the pilot free trade zone and eventually move towards a free trade port. The blockchain depository has been widely piloted under the leadership of three Internet courts in Hangzhou, Beijing, and Guangzhou. With the assistance of blockchain technologies, it has accumulated and stored a large amount of electronic evidence, which has greatly improved the efficiency of case handling and has had a wide-ranging impact.

5 Conclusion

In view of the privacy and security issues and data sharing difficulty in the current judicial system, we employ blockchain technology to construct a certificate deposit system for the Public Security, Procuratorate and Law Division, and selected FISCO BCOS as the underlying platform of the permissioned chain of this system. The upper chain layer, data sharing layer and application enabling layer are the basic framework structure of the system. With the integrated advantages of the blockchain-based public security, procuratorial, judicial and judicial deposit system, data security sharing in the judicial system is realized. While ensuring the rapid sharing of data among various departments, it also ensures the data privacy and security of each department. And with the performance advantages of blockchain, the transparency, immutability and traceability of data on the chain can be achieved. After analysis, the blockchain-based public security, procuratorial and judicial department certificate storage system is of great significance for improving judicial efficiency and reducing judicial costs.

Acknowledgments. This work was supported in part by the Hainan Province Science and Technology Special Fund (ZDYF2020012, ZDYF2021GXJS216), the National Natural Science Foundation of China (62162020).

References

1. Bonomi, S., Casini, M., Ciccotelli, C.: B-coc: a blockchain-based chain of custody for evidences management in digital forensics. arXiv preprint arXiv:1807.10359 (2018)
2. Ichikawa, D., Kashiyama, M., Ueno, T.: Tamper-resistant mobile health using blockchain technology. Jmir Mhealth Uhealth **5**(7), e7938 (2017)
3. Chao, X., Sun, Y., Luo, H.: Secured data storage scheme based on block chain for agricultural products tracking. In: 3rd International Conference on Big Data Computing and Communications (BIGCOM), IEEE, pp. 45–50 (2017)
4. Xu, Y., Shangli, Z., Lanju, K., Yongqing, Z., Shidong Z., Qingzhong, L.: ECBC: a high performance educational certificate blockchain with efficient query. In: International Colloquium on Theoretical Aspects of Computing, pp. 288–304 (2017)
5. Qiao, R., Dong, S., Wei, Q., Wang, Q.: Blockchain based secure storage scheme of dynamic data. Comput. Sci. **45**, 57–62 (2018)
6. Cebe, M., Erdin, E., Akkaya, K., et al.: Block4Forensic: an integrated lightweight blockchain framework for forensics applications of connected vehicles. IEEE Commun. Mag. **56**(10), 50–57 (2018)

7. Ryu, J.H., Sharma, P.K., Jo, J.H., Park, J.H.: A blockchain-based decentralized efficient investigation framework for IoT digital forensics. J. Supercomput. **75**(8), 4372–4387 (2019). https://doi.org/10.1007/s11227-019-02779-9
8. Mohanty, S.P., Venkata, P., Yanambaka, E.K., Deepak, P.: PUFchain: a hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (IoE). IEEE Consum. Electron. Mag. **9**(2), 8–16 (2020)
9. Aitzhan, N.Z., Svetinovic, D.: Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans. Depend. Secure Comput. **15**(5), 840–852 (2016)
10. Aitzhan, N.Z., Svetinovic, D.: Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans. Depend. Secure Comput. **15**(5), (2018)
11. Miyachi, K., Mackey, T.K.: hOCBS: a privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Inf. Process. Manag. **58**(3), (2021)