Research on the Application of Blockchain in Social Insurance Archives

Xiangling Ma[1,a*], Xiangyang Ma[2,b], Anxing Zhao[3,c]

[1]Guangzhou University of Commerce, Guangzhou, 510700, China
[2]Shandong Jianzhu University, Jinan, 250101, China
[3]Guangzhou Baiyun College, Guangzhou,510450, China

[a*]yantaimxl@163.com, [b]mxy@sdjzu.edu.cn
[c]zaxnew@163.com

Abstract. With the advancement of the digitalization of social security archives, these archives face issues related to information resource security. Blockchain technology offers a new approach to addressing the trustworthiness of digital archives. Firstly, the working mechanism of blockchain is analyzed. Secondly, a four-layer architecture model based on the B/S (Browser/Server) model is designed, which includes the Blockchain Layer, Smart Contract Layer, Logic Layer, and Application Layer. A two-tier storage structure for social security archives on the blockchain is designed, utilizing a data storage process of "initial business data on-chain—review—sensitive data secondary on-chain." A collaborative digital signature technology based on trusted timestamps is proposed, where the complete signature is generated from the private keys of Party A and Party B, and the first, second, and third parts of the signature. Finally, it is required to store the digital digest on the public blockchain to enhance the trustworthy management of social security archives.

Keywords: Blockchain; Digital Signature; Digital Archives; Trustworthy Management.

1 Introduction

The Social Insurance Archives Management Regulation is issued by the National Archives Administration and the Ministry of Human Resources in 2009 [1] states: Social insurance business archives are professional textual materials, electronic documents, charts, audio-visual materials, and other historical records on different media, directly formed by social insurance agencies during the handling of social insurance business. Social insurance archives are crucial proofs for individuals to enjoy social welfare and are important information resources for the smooth operation of social security work. They are characterized by a wide variety, massive information volume, long storage cycles, and broad involvement of individuals. These archives include a large amount of sensitive business data and personal privacy data, directly related to personal interests.

K. Zhang et al. (eds.), *Proceedings of the 4th International Conference on Management Science and Software Engineering (ICMSSE 2024)*, Advances in Engineering Research 244,
https://doi.org/10.2991/978-94-6463-552-2_8

Therefore, in the management of social insurance archives, it is essential to ensure the authenticity, accuracy, security, and integrity of archival information.

Since the digital construction of social insurance archives management began, the use of electronic archives has effectively reduced the damage and loss of traditional archives but has also faced data security issues. Moreover, social insurance archive information systems typically transmit and store data in plain text, making them susceptible to theft or illegal tampering, leading to data breaches. These systems also involve operations such as information release, review, and approval. In the event of a data security incident, it is difficult to trace these critical operations, potentially causing severe consequences for the trusted management of social insurance archives.

Blockchain technology, as an emerging distributed technology, provides a fully traceable and tamper-proof management environment by recording archive operations on the blockchain [2]. Therefore, blockchain technology is considered an ideal tool for addressing the challenges of trusted digital archive management.

2 Blockchain Trustworthy Working Mechanism

Blockchain is an application model of distributed data storage characterized by decentralization, traceability, immutability, and transparency [3].

2.1 Blockchain Structure

A block is the basic unit of a blockchain, consisting of a block header and a block body. The block header contains information such as the hash value of the previous block, the hash value of the current block, a timestamp, and more[4] [5]. The block body includes the detailed data within the block. Each block saves the hash value of the preceding block, creating a relationship between blocks, which forms the chain [6]. The blockchain stores transaction records and state changes data. It is a shared and tamper-proof ledger, where each transaction is recorded as a "block". These blocks are connected in sequence, forming a data chain as the data moves from one place to another [7]. Each new data block added strengthens the verification of the previous block, enhancing the validation of the entire blockchain.

2.2 Distributed Ledger Technology

All network participants have access to the distributed ledger and the immutable record of transactions [8]. With this shared ledger, transactions are recorded only once, eliminating the typical duplication of effort in traditional business networks, thereby improving efficiency.

2.3 Immutable Records

Once data transactions are recorded in the shared ledger on the blockchain, no participant can alter or tamper with the information. If a transaction record contains an error, it can only be corrected by adding a new transaction, and both transactions will be visible. All network members must agree on the accuracy of the data, and all verified transactions are permanently recorded, ensuring they cannot be altered, which enhances security.

2.4 Smart Contracts

To accelerate transactions, blockchain stores a set of self-executing rules called smart contracts [9]. By sharing a distributed ledger among network members, time wasted on reconciling records is avoided, resulting in higher efficiency.

3 Research on Trustworthy Management of Social Insurance Archives Based on Blockchain

By leveraging blockchain's anti-tampering mechanisms, trust mechanisms, consensus mechanisms, traceability, and smart contract functionalities, it is possible to ensure the security of metadata, information storage, and utilization, while addressing issues found in traditional management of social insurance archives. This includes user identity verification, information monitoring in archive management, data authentication, and maintenance.

3.1 Design of Trustworthy Management Architecture for Social Insurance Archives

The architecture design of the trustworthy management system for social insurance archives based on blockchain is shown in Fig. 1. The design is based on the server/client B/S model and consists of four layers: blockchain layer, smart contract layer, logic layer, and application layer [10]. The application layer primarily includes the front-end user interface, which is responsible for providing a visual Web interface and handling user requests such as login, file upload, download, and query. The logic layer is the core functional implementation part of the system, which needs to provide implementation methods for corresponding modules based on the functional interface provided by the application layer, such as encoding/decoding, data storage, node partitioning, node selection, and hash value comparison. The smart contract layer is deployed on Ethereum and serves as the main channel for internal contract payments. It is mainly responsible for mapping the data processing results of the logic layer to the storage area of the blockchain layer, facilitating data interaction such as system authorization, query, upload, and download. The blockchain includes the block header and block body. The block body stores core metadata such as file number, title, creation time, and digital summary, while the block header contains information like timestamp, hash value, and access permissions. The blockchain layer is the decentralized database , responsible for storing data generated selected networks and encryption algorithms.

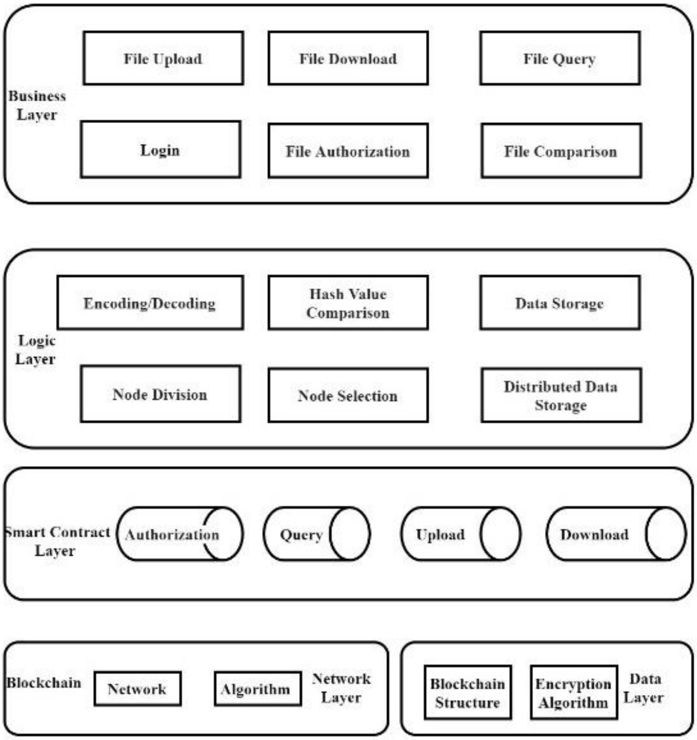

Fig. 1. Design of the Trustworthy Digital Archive Management System Architecture Based on Blockchain

3.2 Two-Level Storage Structure Design for Social Insurance Archives Blockchain

The trustworthy management system for social insurance archives features a social insurance center as the main entity, involving multiple trusted parties and joint maintenance by on-chain entities. Therefore, a blockchain consortium chain system led by the government and the social insurance center is selected. The entities on the chain include the government, social insurance center, social insurance archive filers, medical institutions, and employers. The roles of each entity in the consortium chain are as follows: the social insurance department is the creator of the consortium chain, responsible for establishing the blockchain and authenticating node additions, ensuring that the nodes joining the blockchain are trusted, and assigning appropriate permissions to different entities to jointly operate and maintain the social insurance archive data on the blockchain.

The business data of social insurance archives are classified based on their sensitivity. Personal privacy data and sensitive business data are classified as sensitive data and must be encrypted and stored on the chain. The social insurance archive information system is designed with a two-level storage architecture, building a multi-distributed node blockchain, including operations such as smart contract module design, sensitive data identification, local database establishment, sensitive data ledger creation, and Hyperledger client setup. The two-level storage technology for the social insurance archive information blockchain is shown in Fig. 2. It adopts a data storage process of "business data first on-chain—review—sensitive data second on-chain." Non-sensitive business data are first put on the chain, and after being processed by the smart contract module and sensitive data identification, they can be stored in the local database. Sensitive data are put on the chain a second time and stored in the sensitive business data ledger.

Due to the distributed ledger technology of blockchain, each block has limited space, so each piece of electronic archive information must be selectively put on the chain, such as core metadata reflecting archive information, digital summaries, and data involved in archive operations. By utilizing the two-level storage technology of blockchain, and through smart contracts and consensus mechanisms on multiple distributed nodes, the immutability of social insurance archive information data is ensured. This ultimately realizes a hierarchical storage architecture for the social insurance archive information system based on blockchain technology, thereby ensuring the security of various types of information data in social insurance archives.

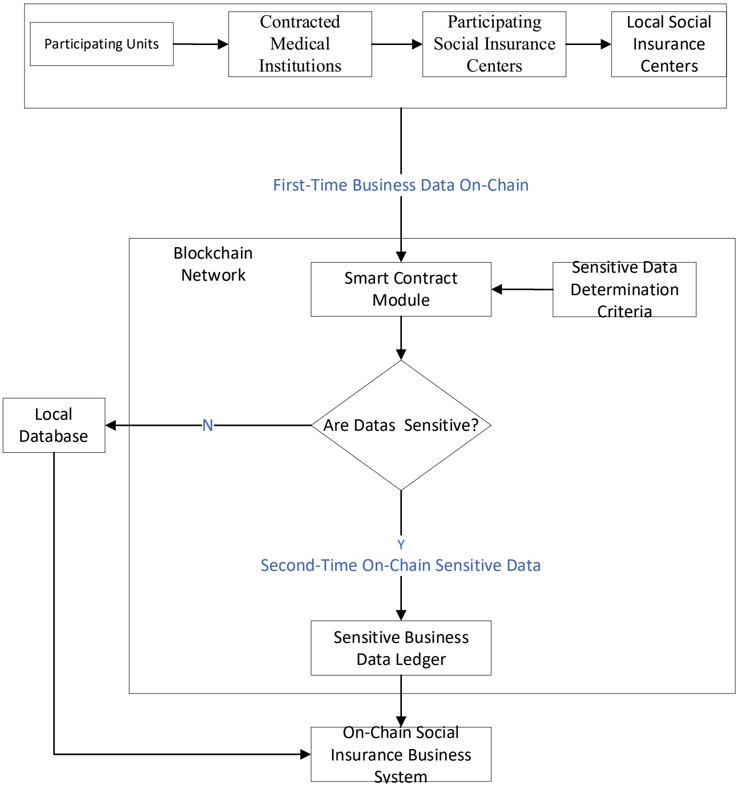
Participating Units
Contracted Medical Institutions
Participating Social Insurance Centers
Local Social Insurance Centers
First-Time Business Data On-Chain
Blockchain Network
Smart Contract Module
Sensitive Data Determination Criteria
Are Datas Sensitive?
N
Local Database
Y
Second-Time On-Chain Sensitive Data
Sensitive Business Data Ledger
On-Chain Social Insurance Business System

Fig. 2. Two-Level Storage Technology of Social Insurance Archive Information Blockchain

3.3 Collaborative Digital Signature Technology Based on Trusted Timestamps

Trusted timestamp technology associates reliable date and time with specific electronic data through the signature of a timestamp server. The user generates the digest data of the file to be signed and submits it to the timestamp server for a signature request. The timestamp server responds with a signature that includes the signature time, proving that the data existed at that specific point in time and has not been altered [11]. The working principle of trusted timestamp technology is shown in Fig. 3. The user sends a hash value to the timestamp service center to apply for timestamp service. The timestamp service center, interfacing with the authoritative time source from the National Time Service Center [12], binds the hash value with real-time information, digitally signs it, and returns the user a timestamp certificate and timestamp file. The user associates the timestamp certificate and timestamp file with the electronic file, forming an electronic file package that can be saved and checked at any time to verify whether the electronic file has been tampered with.

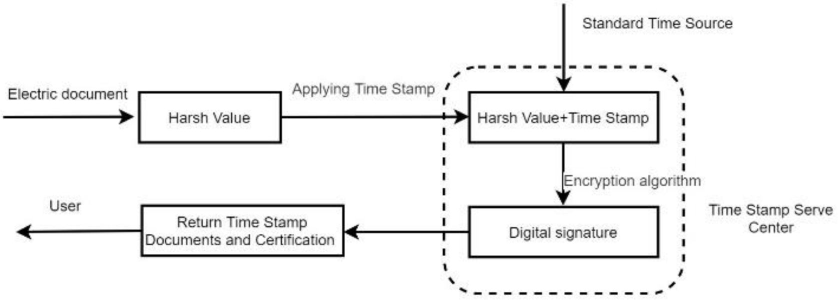

Fig. 3. Working Principle of Trusted Timestamp Technology

A digital signature is an asymmetric cryptographic algorithm composed of a private signing key and a public signing key, where the private signing key must be kept confidential. The public signing key can be disclosed and is usually published in the form of a digital certificate. The signer uses the private key to encrypt the hash value of the data to be signed, and the resulting output is the digital signature. This result can only be verified using the signer's public key. Digital signature technology is widely used to confirm the integrity of the data to be signed, the authenticity of the signer's identity, and the non-repudiation of the signing act.

To address the issues of the uniqueness, trustworthiness, and secure identifiability of identity credentials faced by digital social insurance archives, a combination of digital signature technology and "collaborative digital signature + timestamp" dual identity authentication is employed to enhance the security and convenience of the signing process. The difference between this technology and traditional digital signature technology lies in the generation process of the signing keys and signature values. The private signing keys are independently generated and securely stored by both parties involved in communication, while the public key is computed and published by the server based on a temporary public key generated by the client. During signature computation, both the server and client use their respective signing keys. Each party independently computes their own signature results and then exchanges data with each other, ultimately allowing the client to complete the digital signature generation. This scheme combines the one-to-one correspondence security characteristics of private and public signing keys, effectively ensuring the uniqueness, trustworthiness, and secure identifiability of identity credentials.

The process of collaborative digital digest technology in the trusted social insurance archive system is shown in Fig. 4. According to cryptographic principles, Party B generates a random number and uses Party B's private key to generate the first part of the signature. Before transmitting the electronic file, Party A generates the digital digest of the message to be signed and the random number, uses Party A's private key to generate the first part of the signature, and sends the message digest and the first part of the signature to Party B. Upon receipt, Party B generates a random number, generates the second part of the signature accordingly, and continues to use Party B's private key to generate the third part of the signature and sends it to Party A. Subsequently, Party A generates the complete signature based on the private keys of both parties and the first, second, and third parts of the signatures.

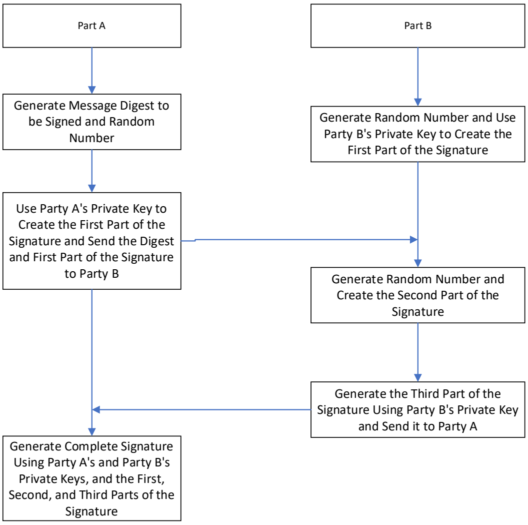
Part A
Part B
Generate Message Digest to be Signed and Random Number
Generate Random Number and Use Party B's Private Key to Create the First Part of the Signature
Use Party A's Private Key to Create the First Part of the Signature and Send the Digest and First Part of the Signature to Party B
Generate Random Number and Create the Second Part of the Signature
Generate the Third Part of the Signature Using Party B's Private Key and Send it to Party A
Generate Complete Signature Using Party A's and Party B's Private Keys, and the First, Second, and Third Parts of the Signature

Fig. 4. Collaborative Signing Logic Between Party A and Party B

3.4 Blockchain Network Design for Trusted Management System

There are various ways to establish a blockchain network, such as public, private, permissioned, or consortium-based [13]. A public blockchain is open to everyone but requires significant computational power, offers low or no transaction privacy, and has weaker security. A private blockchain network is managed by a single organization that decides who can participate in the network and execute the consensus protocol, maintaining a shared ledger. This significantly enhances trust and confidence among participants and can be run behind the organization's firewall or hosted internally. A permissioned blockchain network imposes restrictions on who can participate and perform specific transactions, requiring participants to be invited or granted permission to join. A consortium blockchain involves multiple organizations jointly maintaining the network [14], with pre-selected organizations deciding who can submit transactions or access data.

To maximize the effectiveness of blockchain technology in the trusted management of social insurance archives, digital digests should be stored on a public chain rather than a consortium or private chain, as public trust would be significantly reduced otherwise [15]. Additionally, building and maintaining a consortium or private chain instead of using an existing mature public chain would greatly increase costs. In constructing the blockchain application for social insurance archives, a comprehensive security strategy must be developed, utilizing cybersecurity frameworks, guaranteed services, and best practices to mitigate risks from attacks and fraud. Using blockchain command tools, relevant accounts for the blockchain layer are created during operation to meet the blockchain platform's smart contract functionality requirements and generate public key addresses. Simultaneously, digital digests are stored on the public chain of the social insurance archive blockchain network, ensuring the reliability of social insurance archive information sources using blockchain's immutability and decentralization.

The trusted management system for social insurance archives integrates the generation, management, and utilization of social insurance business archives. Permissions are set based on the job responsibilities of social insurance archive staff, full-time and part-time archivists, and clients. By comparing data on the blockchain with original information in the archive management system, the trusted archive management system ensures that information is genuine and complete throughout the formation, management, and utilization processes. In the trusted management platform for social insurance archives, the design of the archive data management ledger should ensure consistency across nodes at social insurance centers and medical institutions, allowing participation in generating, updating, and storing blockchain operations. When deploying nodes for social insurance centers, participating units, and medical institutions, the advantages of blockchain technology are utilized, and each node department backs up archive information. If an independent node suffers a network attack and fails, the platform's stable operation can still be ensured, achieving secure storage of archive information.

4 Conclusion

The application of blockchain technology to address the trusted management of social insurance archives is a proactive exploratory practice. By recording social insurance archive operations on the blockchain, a fully traceable, immutable trusted management system is provided. The architecture design is based on the server/client model, consisting of four layers: blockchain layer, smart contract layer, logic layer, and application layer. By judging and storing sensitive data on multiple distributed nodes, the immutability of social insurance archive information data is ensured, ultimately achieving a two-level storage architecture for the social insurance archive information system based on blockchain technology, thereby ensuring the security of various types of information data in social insurance archives. Additionally, with the collaborative digital signature and timestamp protection between parties, the trusted authentication significantly improves the accuracy of archive information stored within the blockchain, enhancing application efficiency. Under the decentralized multi-center system of blockchain, social insurance centers and related departments store social insurance archive data in the public chain. Through mutual trust verification among blockchain nodes, data security and stability are effectively ensured, creating a trusted management system for social insurance archives.

References

1. https://www.saac.gov.cn/daj/yaow/201509/cfc5cf5f12a64d9da864eb30c781b7c3.shtml.
2. Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security, 1(1), 36-63.
3. Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. In Conference on the Theory and Application of Cryptography (pp. 437-455). Springer, Berlin, Heidelberg.
4. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin.
5. Zeng, Xiaoyun. Digital Signature Technology in Blockchain Applications [J]. Digital Technology and Applications, VOL38 (8), 2020.8, 176-178.
6. Gao, Shan. Research on Trusted Timestamps for Electronic Document Evidence [J]. Yunnan Archives, 2022.2, 56-58.
7. Zhou, Feng, & Lv, Dongwei. Preliminary Exploration of "Smart+" Archive Management [J]. Beijing Archives, 2019(9), 39-41.
8. Mao, Xiaole et al. Design and Implementation of Electronic Data Evidence Preservation Based on Blockchain [J]. ZTE Communications Technology, 2018(6), Vol.24, 28-34.
9. Wang, Xiaoqi. Research on Centralized Management of Digital Resources under Blockchain Technology [J]. Sichuan Social Insurance Archives Journal, 2024(3), 63-68.
10. Fan, Yingyin, Deng, Peizhen, & Ye, Li. Applicability Study of Blockchain in Digital Resource Sharing of Social Insurance Archives [J]. Sichuan Social Insurance Archives Journal, 2023(1), 22-27.
11. Zheng, Yang. Application Research of Blockchain in Digital Book Copyright Governance [J]. Social Insurance Archives Work and Research, 2022(12), 31-37.
12. Wei, Dawei, Li, Zhiyao, Liu, Jingjing, et al. Research on Smart Social Insurance Archives Digital Resource Management Based on Blockchain Technology [J]. China Social Insurance Archives Journal, 2022, 48(2), 4-12.
13. Zhang, Lin. Construction and Application of Digital Resource Management System for Social Insurance Archives Based on Blockchain [J]. Digital Social Insurance Archives Forum, 2022(9), 36-41.
14. Li, Yingxin, Guo, Zhen, Zhao, Lei, Fu, Guorui. Network Security Assurance of Social Insurance Archives Information System Based on Blockchain Hierarchical Storage and Domestic Commercial Cryptography Technology [J]. Shandong Science, 2024(4), 1-5. DOI:10.3976/j/issn.1002-4026.20230169.
15. Berdik, D., Otoum, S., Schmidt, N., et al. A Survey on Blockchain for Information Systems Management and Security [J]. Information Processing & Management, 2021, 58(1), 102397. DOI:10.1016/j.ipm. 2020.1023.