10.18686/aitr.v2i3.4405

Research on Data Security Management Strategy Based on Blockchain Technology

Zhu Liang

Shaanxi Railway Institute, Weinan 714000, China

Abstract: With the rapid development of high and new technology, blockchain technology has been applied to information management in many fields and plays an irreplaceable role. Due to its immutable and decentralized characteristics, blockchain technology has become the main way of archival information management, providing a variety of possibilities for archival management. Taking blockchain technology as the starting point, this paper analyzes the relationship between blockchain technology and archival information security, and focuses on the data security management strategy of using blockchain technology in archival information to enhance the security and reliability of archival management.

Keywords: Blockchain technology; Data security; Management strategy

Introduction

In the new era, the traditional file management method can no longer meet the management requirements, and the informatization and digital management method has come to the fore and become the mainstream. In this case, blockchain technology has become the best choice to ensure the integrity and security of archive information due to its special nature. As an emerging technology, there are still certain problems in the actual use of blockchain technology, which affects the efficiency and quality of archival information management. To this end, relevant personnel must conduct in-depth research on blockchain technology, adopt diversified management strategies, strengthen data security, and effectively enhance the security of archival information management.

1. Overview of blockchain technology

1.1 Blockchain technology

Blockchain technology was born in the 21st century and is the underlying technology of Bitcoin, with the main purpose of creating a decentralized digital currency trading system that allows users to conduct single-line transactions without being influenced by third parties [1]. The main characteristics of blockchain technology are openness, transparency, immutability, and security, and it has been called "one of the most promising technologies in the new economy" [2]. Blockchain is composed of interconnected and mutually influencing data blocks, each data block has its role and value, contains a large number of data transaction records, and is linked to the previous data block through a certain technology, maintaining the consistency of information and data, and realizing integrity. Blockchain technology is essentially a shared data platform, users through the review of the platform for data retrieval and use, all information stored in it has the characteristics of non-tampering, traces and traceability throughout the process, ensuring the security of information data.

1.2 Blockchain technology and archival information security

The unique characteristics of blockchain technology are in line with the management of archive information, ensuring the security performance of archive information. Blockchain technology is used in archival information management, so that multiple departments are involved in information management, regularly update and maintain information, and store data information into data modules. In the process of management, these archival information will be permanently compiled into the corresponding blockchain, and professionals will carry out certain maintenance and cannot be tampered with by humans, so as to maintain the authenticity of the data information and ensure the security of the archival information [2]. In addition, blockchain technology usually adopts a distributed system to achieve decentralization, where a large amount of data information is stored at the end of the data chain, and the data does not interfere with each other. In this way, even if there is a problem in the system, it will not affect the internal data, and the data can be recovered through the data blocks of each module when the data is damaged, so as to reduce the scope of the impact of a node problem and ensure the longevity, integrity and authenticity of the archive information storage.

2. Data security management strategy based on blockchain technology

2.1 Select the appropriate blockchain type

There are two main types of blockchain technology, public chains and private chains. Public chain refers to a publicly used link, in which everyone can participate in the mobilization and access to data information, which is usually not controlled and managed by unauthorized individuals, and its link performance and security performance cannot be effectively guaranteed, and there are certain risks. The private chain has certain restrictions, which are controlled by individuals and organizations to ensure the privacy of the link. Compared with private chains, public chains have a stronger degree of decentralization, and private chains have more advantages for data and information privacy management, each with its own advantages and disadvantages. Therefore, in the management of archive information, it is better to choose the private chain for storage of data with strong privacy requirements, sensitive topics and confidential information to ensure the security of data.

The private chain can achieve better control and management, so that the stored data and information meet the relevant national requirements and standards, and can formulate a targeted and accurate blockchain according to the actual file information needs. However, it should be noted that the concentration of private chain is much higher than that of public chain, which increases the difficulty and risk of archival information management, and the corresponding permission chain needs to be restricted in the application. The permission chain combines the advantages of private chain and public chain to achieve decentralization and strong control to ensure the quality of file management. In the authority chain, only a small number of authorized staff can operate and manage, such as creating blocks, verifying information, etc., to ensure the security of file information. In addition, in order to ensure the integrity of the archive data, the blockchain with a reliable consensus mechanism can be selected in combination with the management standards to ensure that the archive information remains unchanged for a long time after entry, effectively resist various attacks, and ensure security.

2.2 Use encryption algorithms for protection

When the archives management department uses blockchain technology, it needs to use appropriate encryption algorithms to protect all kinds of confidential documents and information data to avoid others from entering and viewing the archive information without permission. In the case of archives management, multi-signature technology should also be used for file management for extremely important, rigorous and sensitive data information, and multiple keys should be used for protection to achieve the reliability and security of file decryption. In the process of archival information transmission, we should also pay attention to the security and integrity of data, and take end-to-end encryption protection measures to ensure that the entire process of archival information sending and receiving is always encrypted, so as to prevent the leakage of data information during transportation.

In specific practice, the archives management department should evaluate the advantages and disadvantages of different plus technologies, select scientific and reasonable encryption technologies based on the characteristics and requirements of archival information, ensure the feasibility and adaptability of the technology, and effectively protect the security of archival information. For example, the TLS protocol can protect the security of data transportation, the Internet security protocol can protect the security of network communication, and PKI can restrict the access of customers to ensure data and information security. In the use of PKI, it is divided into two types: public key and private key, the public key is used for encryption, and the private key is used for decryption, and the two cooperate with each other to improve the security of archive information. At the same time, the file management part needs to reasonably divide the relevant resources to achieve the maximum efficiency of the encryption system and ensure data security without affecting the user experience.

2.3 The use of distributed characteristic equipment

In the management of archive information, it is necessary to make full use of the distributed characteristics of blockchain technology, store it on multiple data chain nodes, and do not interfere with each other between data and data, so as to realize the security of data information storage. In order to avoid problems in the process of file management, it is necessary to back up important file materials to prevent data loss.

When designing data backup strategies, archives departments can take advantage of distributed characteristics to set up diversified storage nodes in different blocks and different network environments to avoid the impact of network failures or other factors. Secondly, with the help of sharding technology, the file data in the large-scale state can be reasonably divided into multiple small data information according to the type, and distributed storage on multiple nodes of the blockchain to improve management efficiency and management quality. Finally, distributed backup means that there are two sets of identical data information in the network system, and a consensus algorithm needs to be used to ensure the consistency of the data.

2.4 Establish rules for the operation of smart contracts

When the archives department carries out management with the help of blockchain technology, it is necessary to establish perfect smart

contract operation rules to achieve high-quality and high-level intelligent management and ensure the security of archive information. First of all, it is necessary to develop a scientific and clear access rights system, stipulating the types and requirements of visitors, and clearly knowing who can access and under what circumstances. In this regard, corresponding access standards can be set, and the visiting personnel and access time can be specified to ensure the smooth development of the visit work. Secondly, it is necessary to ensure the integrity and security of data in operation, add verification functions and modification functions, and ensure that the management work complies with laws and regulations. In the verification process, diversified encryption technologies can be adopted to improve the efficiency and accuracy of verification and ensure the integrity of data. Finally, it is necessary to automate the data information processing process. Relevant technical personnel should ensure that the smart contract can perform various compliant operation processes, such as deleting browsing records, saving relevant data, and archiving in a timely manner. If any problems are found in operation, warnings and early warnings can be issued as soon as possible, and management personnel can be notified for inspection and repair, so as to reduce management risks.

3. Concluding remarks

To sum up, the introduction of blockchain technology in file management, with its decentralized characteristics, ensures that file information is not easily tampered with and ensures data security. In this regard, when applying blockchain technology, relevant staff must pay attention to the security of file information, strengthen the security management of data, select the appropriate blockchain type, use encryption algorithms, set up file backup with distributed characteristics, establish smart contract operation rules, and effectively improve the level of file information security management.

References

[1] Wang Qingle. Research on research data security management strategy of university digital library based on blockchain technology[J]. Library Work and Research, 2021, (12):63-69.)

[2] Liu Wenjuan. Archive informatization and data security management based on blockchain technology[J].Lantai Inside and Outside, 2023, (24):14-15+21.)

[3] Jin Lishuang. Heilongjiang Archives, 2022, (04):55-57.)

Project information:

2023 Weinan Public Science Literacy Improvement Program Project "Research on Popular Science Information Service Platform for the Public" No.: WSKS2-017

Shaanxi Railway Engineering Vocational and Technical College Graduate Special Project "Research on Archive Informatization Construction Based on Blockchain Technology" No.: KY2020-11