Research on Information Security Protection Strategy of Digital Archives Based on Blockchain Technology

Qingqing Cao

{caoqingqing08@qq.com}

Officers College of PAP, Chengdu, China

Abstract. The characteristics of blockchain technology have a high degree of compatibility with the characteristics of digital archives, which can provide an innovative approach for information security management of digital archives. In response to information security issues such as distortion, unavailability, and confidentiality of digital archives, literature research, comprehensive analysis, and other methods are used to reveal the risks of authenticity, integrity, availability, and security of digital archives. The application advantages of blockchain technology in digital archive information security protection are deeply explored. Finally, regulatory standards, process management, facility construction Provide emerging security protection strategies for digital archives based on blockchain technology in terms of technology research and development and talent cultivation, further improving the intelligent level of digital archive resource management.

Keywords: Digital Archives;Information Security Protection;Blockchain Technology

1 Introduction

With the continuous improvement of information technology, the form of carrier for storing archive resources has also undergone significant changes. At present, most paper archive resources are converted into digital data, using electronic carriers as a unified medium for processing and storage, and developing towards information digitization and digitization comprehensively. No matter how the carrier form of archives changes, they are an important special resource for the archives themselves and are not renewable. These data stored in archives are extremely important data resources for society and economy. Only by fully mining these data while ensuring their security, can they be more valuable. Once damaged, they will cause significant losses to the country and units. How to effectively ensure the security of archival data is an urgent problem to be solved. Blockchain is one of the Bitcoin application methods, providing new tools for digital archive management.

Blockchain originates from security technology and is essentially a decentralized distributed ledger database that establishes trust mechanisms through cryptographic algorithms. It allows any multiple nodes in the participating system to generate a sequence of time series data blocks using cryptographic methods. Each data block contains all the system information exchange data for a certain period of time, and generates data fingerprints to verify the validity of their information and link to the next database block [1]. In the field of archive management,

ICMEIM 2023, September 08-10, Wuhan, People's Republic of China

DOI 10.4108/eai.8-9-2023.2340190

blockchain technology can help build a more comprehensive digital archive management system, enabling better creation and preservation of digital archives.

2 The Risks of Digital Archives in Information Security Management

Digital archive information security management is to ensure the integrity, availability, and confidentiality of archive information content, protect the hardware, software, and data in the system from accidental or malicious factors that may cause information damage, leakage, or inability to access. However, digital archives are stored on servers, which are similar to other business servers and data security. They are susceptible to hacker attacks from internal and external networks, virus and Trojan infections, and security issues in server hardware and systems can directly affect the security of digital archive information. At present, the risks of digital archives in information security management mainly include the following four factors.

2.1 Difficult to distinguish authenticity

During the collection, transmission, and storage of archives, their authenticity is often susceptible to infringement due to factors such as the use of equipment, archive management systems, operators, and network environment. Firstly, software and hardware devices are unable to correctly recognize the information and image abnormalities of paper archives; Secondly, in the process of management and utilization, digital archive information can be saved on various carriers. Due to the separability of digital archive information between content and carriers, managers and users can use various devices to read and manually modify digital archive information; Thirdly, the current management of digital archives is based on centralized nodes, databases, and servers. When the digital archive information of a certain node is artificially tampered with, the entire system will flow incorrect digital archive information, ultimately leading to problems such as inconsistent content between digital archives and traditional physical archives or fictitious false archives that do not exist.

2.2 Integrity is difficult to guarantee

The integrity of digital archives requires that the content, metadata, archive information packages, information signatures, etc. of the archives are not missing throughout the entire digital archive management lifecycle. However, there are still the following risks at this stage: firstly, due to the untimely and incomplete collection of archives, the content of the archives is missing; Secondly, incomplete collection of metadata information leads to the absence of necessary descriptive items. Metadata is data related to data [2] and is a necessary item for recording digital archives; Thirdly, the number of archived answer files is inconsistent with the metadata records; The fourth reason is that the processing of information such as digital signatures is not standardized, resulting in unrecognizability.

2.3 Availability challenged

The availability of digital archives requires that they can be retrieved and presented. One is that it may be stored on storage media such as disks, which may cause unreadable issues; Secondly, centralized management may lead to unstable query times for digital archives due to network reasons, such as network congestion, resulting in the inability to process and use digital archives in a timely manner; In addition, the inconsistent standards of various digital archive management systems result in information silos, and archive data cannot be connected or shared, which will reduce the availability of archive data.

2.4 Security threatened

With the explosive growth of the number of digital archives, digital archives are facing various risks in storage, retrieval, backup, and other aspects. If a large number of digital archives are easily intercepted and destroyed during the circulation process, it can cause information leakage issues. In addition, some digital archive management systems have not backed up various types of digital archives in a timely manner, resulting in server damage or attacks, making archive data unable to be retrieved.

3 The Application Advantages of Blockchain Technology in Digital Archive Information Security Management

Currently, the architecture of blockchain consists of six layers, namely: data layer, network layer, consensus layer, incentive layer, contract layer, and application layer. For digital archives, hash algorithms based on digital signatures, consensus mechanisms on a distributed basis, and programmable intelligent contracts are important technical guarantees for digital archives. The architecture of blockchain is shown in Fig.1.

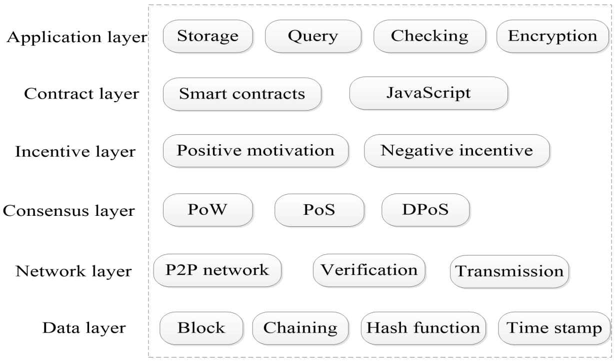

Fig. 1. Blockchain architecture

The architecture model of blockchain starts from the lowest data layer and is the foundation of blockchain. The data in this layer, including blockchain structure, timestamps, public keys, keys, and so on, is stored in this layer. Further up is the network layer, which uses P2P network technology for data exchange and transmission. The consensus layer mainly has three rules: PoW (Proof of Work)[3],PoS(Proof of Stack)[4],and DPoS (Delegated Proof of Stack)[5], responsible for verifying data passing through the data layer. The incentive layer includes both positive and negative incentives. Blocks that violate the system will be punished, while those that contribute to the blockchain will receive rewards. The contract layer utilizes smart contract technology to formulate rules based on the needs of users or managers, solving the problem of distrust between users. The application layer includes the developers of the system to develop various application functions of the blockchain system in this layer. The use of blockchain technology in digital archive information security management has the following advantages.

3.1 Ensure the authenticity of digital archives

The use of traditional electronic signatures in the registration and reception process of digital archives poses problems such as invalid signatures and difficulty in being recognized by the outside world. If we want to meet the needs of digital archives that have been preserved for decades or even permanently, and solve problems such as the expiration of traditional digital signature services, we usually use the method of removing digital signatures, which cannot verify the authenticity of digital archives; Another approach is to retain digital signatures but require regular use of timestamp technology to extend their validity period. Trusted timestamps are issued by the National Timestamp Service Center, verified and recorded jointly by consensus nodes, and information such as digital signature certificates of digital archives is saved on the blockchain, providing verification services to prevent behavior denial and avoid human modification.Save the hash value of digital archives on the blockchain, and the hash algorithm identifier proves the authenticity of the hash operation. The hash value encrypts the information of electronic archives. If someone wants to maliciously tamper with certain information of electronic archives, they need to use force to crack the corresponding hash value. By utilizing technologies such as asymmetric encryption and consensus mechanisms, the authenticity of hash values in digital archives on the blockchain can be jointly maintained, effectively preventing illegal tampering of hash values[6]. The application advantages of blockchain technology in digital archive authenticity protection are shown in Fig.2.

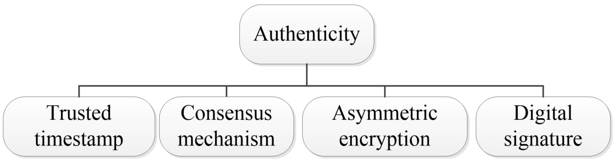

Fig. 2. Authenticity Application Advantages

3.2 Ensuring the integrity of digital archive information content

Through consensus mechanisms and peer-to-peer networks, the archive system has changed from a traditional database format to a "distributed ledger" that is jointly maintained, information shared, and has consensus among all participants. All nodes can participate in checking the number, type, and other information of digital archives [7]. In scenarios such as sending, receiving, and long-term storage, By comparing and verifying whether the hash values stored on the blockchain are consistent with the hash values of local electronic files, the integrity of archive information is ensured. In addition, the blockchain system uses UUID (Universally Unique Identifier) to identify and store relevant information about electronic file business processes, accurately recording the recorded content and ensuring its integrity, achieving traceability of the complete lifecycle of digital archives from formation to destruction or permanent preservation. The application advantages of blockchain technology in digital archive integrity protection are shown in Fig.3.

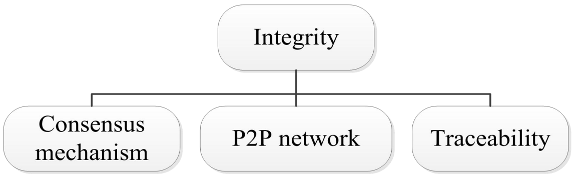

Fig. 3. Integrity application advantages

3.3 Improving the availability of digital archives

In the stage of digital archive collection, smart contract technology in blockchain can be used to avoid human negligence. Smart contract technology automatically executes the protocol formulated by nodes in the chain and completes the collection of electronic archives. For the conversion of digital archive formats, intelligent contract technology can also be used to achieve intelligent automatic conversion of archive formats. In addition, the characteristics of blockchain technology in distributed storage can be fully utilized, and each business organization can be treated as a blockchain node, each storing an identical copy of the blockchain. Even if the information stored by a node is lost, the data of the lost node can be recovered through other nodes, ensuring the long-term availability of digital archives [8].In addition, blockchain technology can ensure the security of electronic file transmission through technologies such as smart contracts and encryption algorithms, without changing the file itself, to prevent electronic files from being tampered with or stolen, and thus ensure the long-term availability of electronic file files. The application advantages of blockchain technology in digital archive integrity protection are shown in Fig.4.

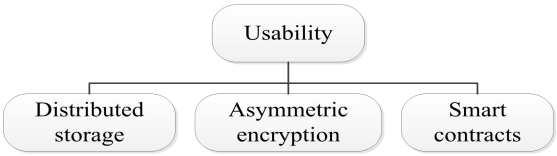

Fig. 4. Usability application advantages

3.4 Protecting the Security of Digital Archives

The distributed storage of blockchain enables digital archives to be no longer limited to traditional centralized storage devices. The storage devices of all nodes on the blockchain can be used as storage devices for the archive system. The distributed storage of blockchain has also changed the centralized form of archive systems, becoming the shared maintenance of multiple nodes in the chain. Even if a node's data is lost or damaged, data recovery can be based on other nodes in the chain, providing a high fault tolerance rate for electronic archives. In addition, different permissions can be granted to different nodes and user groups, including data access permissions, consensus permissions, etc. At the same time, special supervision and audit permissions can also be provided for archive system regulatory agencies to manage risks throughout the entire lifecycle of electronic archives, effectively avoiding illegal access. In addition, using blockchain technology can not only achieve full recording of the movement status of electronic files, but also monitor illegal behavior of tampering with electronic files. When extreme situations such as malicious network attacks and forced tampering with block content occur, such as more than half of the nodes being breached and archive data being tampered with, management personnel can restore the blockchain to its initial state based on its unidirectional chain storage characteristics. The application advantages of blockchain technology in digital archive security protection are shown in Fig.5.

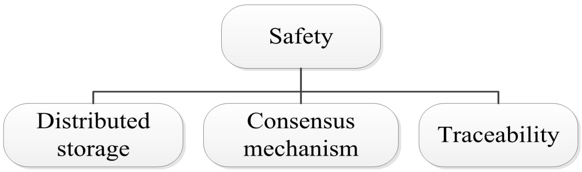

Fig. 5. Safety application advantages

4 Digital Archive Information Security Protection Strategy Based on Blockchain Technology

4.1 Strengthen the construction of digital archives regulations and standards

Without rules, there is no square. For the protection of digital archive information security, it is necessary to introduce blockchain technology and improve corresponding regulations and standards to effectively ensure that blockchain technology can play a role in digital archive information security protection. Improve the quality control standard systems such as the "Digital Signature Specification Based on Blockchain Technology", "Distributed Storage Standard for Archival Data Based on Blockchain Technology", and "File Data Sharing Protocol Based on Blockchain Technology" for the management architecture, system integration, infrastructure, platform docking, and network transmission of blockchain technology applications; To address the issue of digital archive information silos, we will improve the blockchain digital archive resource sharing standards and provide solid institutional guarantees for the sharing and utilization of digital archive resources.

4.2 Strengthen the full process management of digital archives

Blockchain is divided into three categories: public chain, alliance chain, and private chain [9]. The public chain access mechanism is unlicensed and anyone can participate, but its performance is relatively low; The alliance chain access mechanism is licensed and only certain institutions can participate, with high performance; The private chain access mechanism is licensed, and only internal organizations can participate, with the highest performance. Taking alliance chain as an example, blockchain technology is used to protect the security of archive information throughout the entire digital archive management lifecycle, such as archive collection, identification and disposal, organization, preservation, and utilization. This ensures the four characteristics of archive information, namely security, authenticity, integrity, and availability, and achieves full information security protection for electronic archives. The entire process management of digital archives based on blockchain technology is shown in Fig. 6.

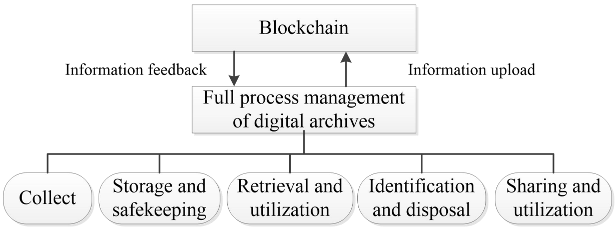

Fig. 6. Full process management of digital archives based on blockchain technology

4.3 Enhance infrastructure construction and technology research and development

On the one hand, it is necessary to strengthen the infrastructure construction of blockchain and equip it with various software and hardware infrastructure equipment required for blockchain; On the other hand, it is necessary to strengthen the research on key technologies of blockchain application in digital archive information security, and choose efficient consensus mechanisms, smart contracts, data naming rules, and data standards. Further technical breakthroughs will be carried out in the quality management of archival data, evidence chain systems, digital voucher systems, and data preservation systems, promoting technological innovation, iteration, and application, promoting real-time monitoring, alarm, tracking, and repair of archival data, and maintaining the authenticity, integrity, trustworthiness, reliability, and safe utilization of archival data.

4.4 Promote the cultivation of archive information management talents

The new generation of information technology is widely used, and the environment, objects, and content of archival work have undergone significant changes. It is urgent to innovate the concept, methods, and models of archival work, accelerate comprehensive digital transformation and intelligent upgrading [10]. Currently, a large number of technologies such as decentralization, asymmetric encryption, and consensus mechanisms are used in digital archives, requiring archive management personnel to have a detailed understanding of the application methods of such technologies, Clarify the application characteristics and shortcomings of this technology [11], proficiently master the application of relevant supporting software in archive information security protection, and improve archive data management skills and blockchain technology application skills through professional learning, special lectures, academic discussions, and practical investigations, truly achieving active adaptation to new technologies, new environments, and new changes, and possessing modern archive information management thinking.

5 Conclusion

In the context of increasingly developing internet technology, while the concept of digital science deepens, the security of digital archive information is increasingly valued, and archive management needs to keep pace with the times. Especially with the acceleration of archival informatization process and the continuous updating and iteration of data management technology, as well as the support of emerging technologies such as big data, cloud computing, artificial intelligence, and blockchain technology, the ability to manage archival information security continues to improve. Introducing blockchain technology into the information security management of digital archives is a positive and beneficial exploration, which not only ensures the authenticity and security of collected archive information, but also strengthens the effective utilization of archive information. This not only makes archive management services more efficient and reliable, but also enhances the intelligent level of digital archive resource management. However, blockchain technology still has some shortcomings, such as the emergence of consensus risks, limited scope, lack of regulatory experience, and high development costs. The next step is to deeply integrate modern emerging technologies with archive management work, promote the modernization of archive management, and reconstruct the information ecological structure of archive management.

References

[1] Kammoun M, Elleuchi M, Abid M, et al. HW/SW Architecture exploration for an efficient implementation of the secure hash algorithm SHA-256. Journal of Communications Software and Systems, 2021, 17(2):87-96.

[2] Cui Hongli.Application of Block Chain Technology in Electronic Archives Management. Lantai World,2023(5):107-110.

[3] Tschorsch F, Scheuermann B. Bitcoin and Beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 2016, 18(3):2084-2123.

[4] Zhong Zengsheng An improved research on blockchain PoS consensus algorithm.Journal of Chongqing Business University: Natural Science Edition, 2021, 38 (04): 36-41.

[5] He Shuai, Huang Xiangnian, Liu Qianbo. Research on the Improvement of DPoS Blockchain Consensus Mechanism. Computer Application Research, 2021, 38 (12): 3551-3557.

[6] Hai Xiao.Research on the Strategy of Information Security Construction of Digital Archives Based on Block Chain Technology.Shanxi Archives,2020(4):118-124.

[7] Chen Xiaohui. Relevant Standards for Electronic Archive Management in China. Lantai World, 2018 (03): 25-32.

[8] Yu Zhiying, Yu Yingxiang. Applicability and Path Analysis of Blockchain Technology in the Maintenance of Electronic Document Four Properties. Shanxi Archives, 2021 (01): 27-34.

[9] Zhou Meng, Li Yong. Analysis of the Application of Blockchain Technology in the Field of Bank Payment and Clearing. Financial Horizon, 2018 (06): 81-88.

[10] The State Administration of the People's Republic of China issued the "14th Five Year Plan for the Development of National Archives" . Archives of China, 2021 (6): 18-23.

[11] Jin Bo, Sun Yao, Yang Peng. Research on Quality Assurance of Archival Data Based on Blockchain Technology . Library Journal, 2023 (7): 1-15.