Hindawi
Scientific Programming
Volume 2021, Article ID 2613656, 7 pages
https://doi.org/10.1155/2021/2613656

Research Article

Blockchain Technology for Management of Intangible Cultural Heritage

Shen Lvping

Department of Arts, Shaoxing University of Arts and Science, Shaoxing, China

Correspondence should be addressed to Shen Lvping; shenlvping@usx.edu.cn

Received 1 October 2021; Revised 14 November 2021; Accepted 20 November 2021; Published 3 December 2021

Academic Editor: Jamil Hussain

Copyright © 2021 Shen Lvping. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the development of information technology and network technology, digital archive management systems have been widely used in archive management. Different from the inherent uniqueness and strong tamper-proof modification of traditional paper archives, electronic archives are stored in centralized databases which face more risks of network attacks, data loss, or stealing through malicious software and are more likely to be forged and tampered by internal managers or external attackers. The management of intangible cultural heritage archives is an important part of intangible cultural heritage protection. Because intangible heritage archives are different from traditional official archives, traditional archive management methods cannot be fully applied to intangible heritage archives' management. This study combines the characteristics of blockchain technology with distributed ledgers, consensus mechanisms, encryption algorithms, etc., and proposes intangible cultural heritage file management based on blockchain technology for the complex, highly dispersed, large quantity, and low quality of intangible cultural heritage files. Optimizing methods, applying blockchain technology to the authenticity protection of electronic archives and designing and developing an archive management system based on blockchain technology, help to solve a series of problems in the process of intangible cultural heritage archives management.

1. Introduction

Culture cannot be abridged to the tangible items as it is living and continuously evolving and essentially is composed of the elements that represent the living culture of humans, referred to as "intangible cultural heritage." This includes the various aspects of cultural heritage such as traditions and living expressions inherited from ancestors and covers a wide range of cultural values and norms such as arts, social practices, rituals, beliefs, and events [1]. With the development of computer technology and the improvement of economic levels across the world, different data intangible cultural heritage management systems have been widely used in the management of intangible cultural heritage. The traditional intangible cultural heritage management methods such as using paper archives have the disadvantages of slow search speed and complicated management process. The digital intangible cultural heritage management system can speed up the retrieval and monitoring of intangible cultural heritage through database query, simplify the management process of intangible cultural heritage through online approval, reduce labor costs, and improve office efficiency [2]. Currently, intangible cultural heritage is difficult to collect, identify, and monitor. Therefore, management of the intangible cultural heritage has gradually attracted attention. How to protect the authenticity and security of intangible cultural heritage documents so that they cannot be easily stolen, tampered with, or destroyed has become a hot issue in the field of digital intangible cultural heritage construction. Blockchain is a distributed ledger technology that is decentralized, does not require trust, and has strong anticalculation modification [3]. It uses a variety of computer technologies such as cryptography, probability theory, consensus mechanisms, and distributed networks. Blockchain technology was first applied to the Bitcoin blockchain and there are thousands of distributed nodes around the world which have been running uninterruptedly for nearly 10 years, yet no major events have occurred [4]. Although

blockchain technology originated from encrypted digital currency, its development and application are not limited to the financial field, but can be widely used in many fields such as culture and entertainment, social welfare, and data protection [5]. Blockchain's decentralization, strong anticalculation modification, and information traceability are very suitable for intangible cultural heritage protection scenarios. Although blockchain technology has many advantages, it still has problems such as low access efficiency and high economic cost. Blockchain cannot replace the existing database technology, but is often used as a supplementary technical means in combination with other technologies. In summary, the existing intangible cultural heritage management systems generally have problems such as poor security, easy calculation changes, and destruction. This article comprehensively utilizes multiple technologies such as blockchain and system monitoring and studies and designs based on districts. The intangible cultural heritage management system of the blockchain can effectively and better protect a country's outstanding intangible cultural heritage.

2. Related Work

Blockchain is a decentralized, no need to trust, and tamper-proof distributed ledger technology [6], derived from Bitcoin's white paper [7], which comprehensively utilizes cryptography, probability theory, and consensus mechanisms. Various technologies such as distributed networks are expected to solve the problems of poor data security and weak anticalculation modification that are common in existing file management systems. In recent years, many experts, scholars, and related organizations at home and abroad have continued to explore and practice blockchain technology in data protection and sharing. The Proof of Existence project [8, 9] realized the authenticity protection of electronic files by storing the hash value of the file in the blockchain transaction record. The project implemented the data protection of electronic files, but the data protection function is relatively simple and the cost is relatively high. The chain point project [10] implements a universal electronic file protection method based on the Bitcoin blockchain, which reduces the cost of data protection by calculating the hash value of the file and then constructing and storing the Merkel tree [11]. However, there is a lack of correlation between the data, and data recovery cannot be achieved. Azaria et al. [12] used smart contracts to build a decentralized medical data access and permission management system. This system realized the ownership of the patient's medical data and enabled the patient to independently share medical records. However, the system relies on a centralized database for data storage and lacks the protection of the private blockchain by the public blockchain which is open to public and everyone can join it. The domestic Ant Financial Company uses blockchain technology to record the specific flow of Alipay's donations and realizes the openness, transparency, traceability, and noncorrection of the use of the donations [13]. The blockchain team in this laboratory has also been committed to the research of blockchain technology in data protection and has practiced in multiple application scenarios such as sampling robots and medical data protection [14, 15].

In summary, we design and develop a blockchain-based intangible cultural heritage management system, using the strong antitampering and decentralization features of the blockchain, through the summary information of the intangible cultural heritage information on the chain. The storage method can realize the protection and verification of the intangible cultural heritage data in the management system and effectively solve the general security problems in the existing intangible cultural heritage system [16–18].

3. Method

In this section, we are going to discuss the system architecture of the proposed system in detail and the other modules including system monitoring platform, server status monitoring module, and notification module.

3.1. System Structure. The file management subsystem is developed using Microsoft's.NET platform. It adopts the object-oriented development method, the design principle of "high cohesion and low coupling," and the design method of three-tier system architecture. It consists of system interface layer, business logic layer, and data access layer. The access layer consists of three parts. As shown in the figure, the interface layer is the bridge between users and the system, providing users with a friendly operation interface, which can transform user operations and inputs into specific requests and pass them to the logic layer. The business logic layer is the bridge between the interface layer and the data access layer. It converts user input and requests at the interface layer into specific business processes and performs data access operations through the data access layer. The data access layer realizes local data access through database calls and accesses data from the blockchain data protection subsystem through RESTful interface calls which is shown in Figure 1.

3.2. System Monitoring Platform Architecture. The design goal of the system monitoring platform is to be able to monitor the running status of all server hosts and applications of the blockchain-based file management system, to collect and process abnormal and error information that occur during the execution of the program, and to be able to guarantee the stability of the system, including the stability of the monitoring platform itself and the application program. The system monitoring platform can be divided into two parts: server status monitoring and application error monitoring. The server status monitoring is mainly realized through the open source Zabbix monitoring solution [19]. The monitoring information in the target server is collected through the Zabbix Agent client, and the information is sent to the Zabbix Server by means of active reporting. Application error monitoring is performed on the application through the HTTP interface, the error information in the system is collected, and the corresponding alarm strategy is implemented and shown in Figure 2.

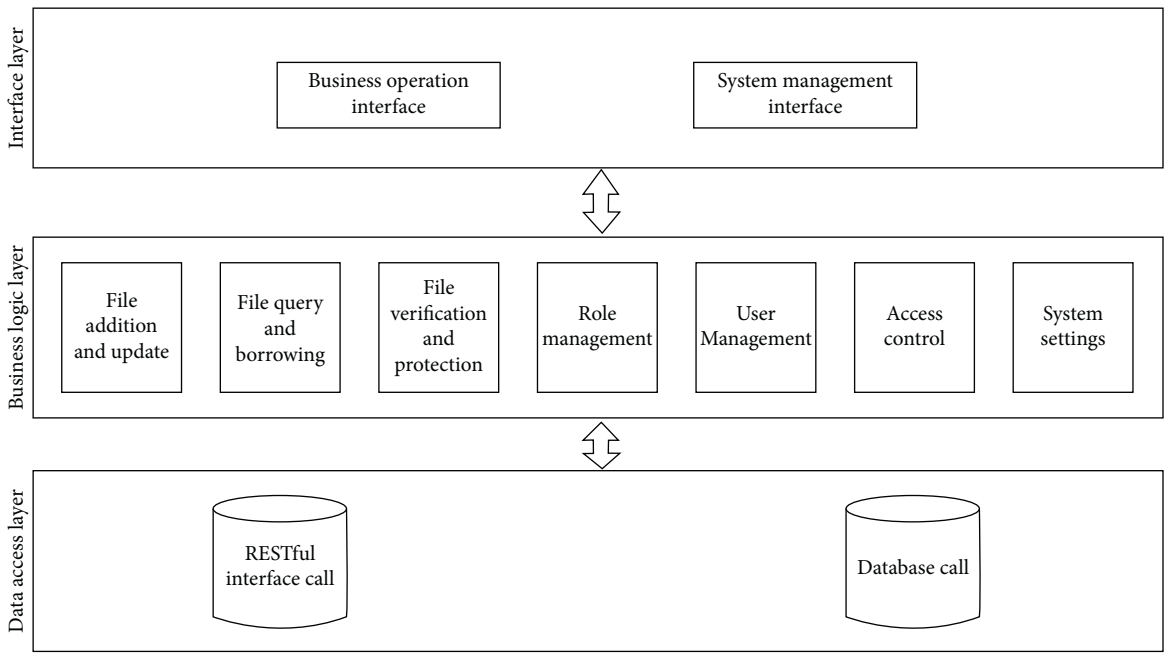

Figure 1: File management system architecture.

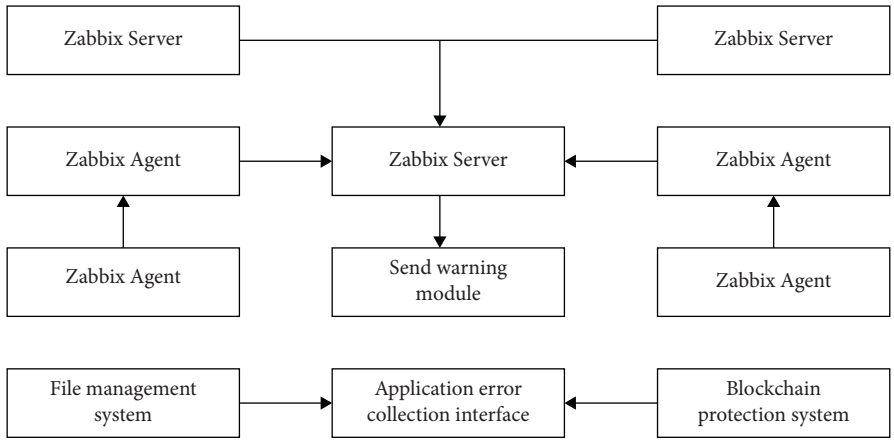

Figure 2: System monitoring platform architecture.

3.3. Server Status Monitoring Module. Server status monitoring is the core module of the monitoring platform, including the monitoring of the hardware parameters and software operating status of the server host. The Zabbix Agent client has two working modes, active monitoring and passive monitoring. Active monitoring means that, after the Zabbix Agent client collects the information of the monitoring target, it actively establishes a TCP connection with Zabbix Server and transmits monitoring information. In passive monitoring, after the information collection is completed, the Zabbix Agent client does not actively send information, but waits for the Zabbix Server to establish a connection with it and then transmits the monitoring information. For economic cost and security considerations, most server hosts run in a local area network environment and do not have public IP addresses, and different servers may also exist in different local area networks. Therefore, in order to monitor all target servers, this module adopts an active monitoring structure, as shown in Figure 3. You only need to configure a public network IP for one server of Zabbix to achieve distribution in different geographic locations and network areas. For server monitoring, we first install the Zabbix Agent client on each server to collect monitoring information, then deploy a Zabbix Proxy program for each local area network to collect and summarize the monitoring information, and finally establish a TCP connection with Zabbix Server through the public IP of the Zabbix Server and report to the monitoring information.

3.4. Warning Notification Module. In the system monitoring platform, sending alarm notifications is a very important step. Whether the error information can be transmitted to relevant personnel in an effective way in a timely manner will

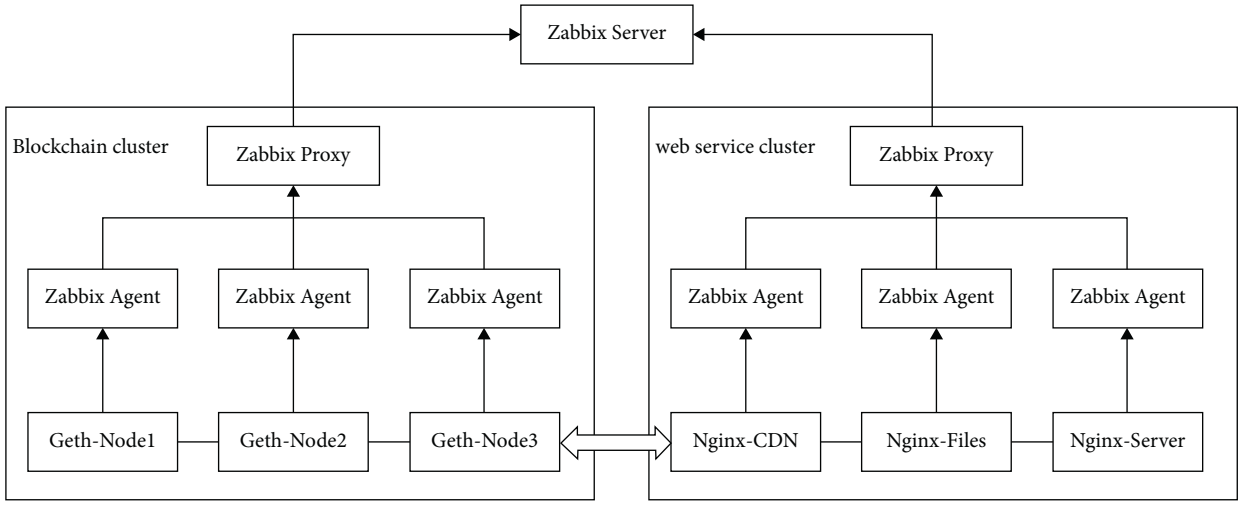

Figure 3: Active monitoring module structure.

affect the robustness and stability of the entire blockchain-based file management system. The alarm method of the system monitoring platform should have the characteristics of safety, efficiency, and low price. In addition, it should have multiple alarm methods to complement each other to avoid the failure of a certain alarm method or the situation that it is not checked in time. The system monitoring platform implements four alarm methods: e-mail, SMS, WeChat social app, and QQ social app [20]. The administrator can select one or more alarm methods when configuring alarm rules. When a certain alarm method fails, other alarm methods will be automatically used as a substitute, and the monitoring platform administrator is notified. E-mail is a commonly used warning method, which has the advantages of simple operation and low economic cost. Compared with the e-mail alert operation, SMS alert is a more efficient and direct alert method, but it needs to be sent with the help of a third-party SMS operator, and it needs to be paid for. With the continuous development of the mobile Internet, social networking apps such as QQ and WeChat have gradually become popular, and sending alert notifications through social software has become a good supplementary method.

4. Experiments and Discussion

4.1. Block and Blockchain. The block is the basic part of the blockchain. It records all transaction records in the blockchain during the creation period and records the address of the previous block in the block header. In this way, it forms a one-way chain structure in the blockchain [17]. The structure of the block is shown in Table 1.

Each block includes five fields: block header, block size, magic number, transaction quantity, and transaction [21]. The transaction field records a list of specific transaction information. The magic number is a fixed value. The block header field is the abstraction of all transaction content in a block and is the key to building a blockchain. The structure of the block header is shown in Table 2.

4.2. Blockchain-Based Data Storage Solution. Blockchain is a decentralized data storage method that has the advantages of no trust, irreversible data, and nontampering. However, in the actual application process of the project, it is still necessary to solve the problems of low data access efficiency and high economic cost. There are two ways to store data in the blockchain through the OP_RETURN field of the transaction and the smart contract to store data. This article chooses to use the smart contract for data storage because the smart contract has a richer data organization form, and there is no OP_RETURN field 40 bit size length limit. Whether it is the OP_RETURN field in the blockchain or the storage of information in the smart contract, it is realized in the form of transactions. Therefore, every time you write data, you need to pay a certain amount of digital currency as the transaction fee. The transaction fee and writing size of the input data are proportional, and the write operation needs to be completed after the corresponding block is packaged by the miner. According to statistics from the ethgasstation.info website, at the time of writing this article, the average transaction fee of Ethereum is 2Gwei, which is 0.2 yuan in RMB (Ren Min Bi). The file management subsystem often performs file addition and modification operations, and from Figure 4, we see the transaction cost of data writing is undoubtedly very high.

This paper studies the file management in the intangible cultural heritage as an example. Based on the consideration of the above problems, this paper designs a data storage scheme combining public chain, private chain, database, and IPFS (interplanetary file system) cluster. The solution uses IPFS to store the specific content of each file (including file attributes, attachment attributes, and original text of the attachment), the private chain stores the IPFS address and digital fingerprint of each file through smart contracts, and the public chain stores the blocks of the private chain through smart contracts. The height and hash value are shown in Figure 4. Since the file information in the private chain can only be queried by the file number and the file content in the IPFS can only be queried by the IPFS address, the solution also uses the current attributes of the MongoDB

Table 1: Block structure table.

Field	Size (bytes)	Description
Block header	80	6 fields in the block header
Block size	4	Block size
Magic number	4	Fixed value 0xD9B4BEF9
Transaction counter	1–9	The number of transactions contained in the block
Transaction	Transaction size	List of transactions included in the block

Table 2: Block header field table.

Field	Size (bytes)	Description
Version	4	System version number
Previous block hash	32	Previous block hash
Nonce	4	The parameters that generate the target hash value
Hash Merkle Root	32	Hash value of all transactions
Bits	4	Proof of work standards
Timestamp	4	UTC timestamp of block generation

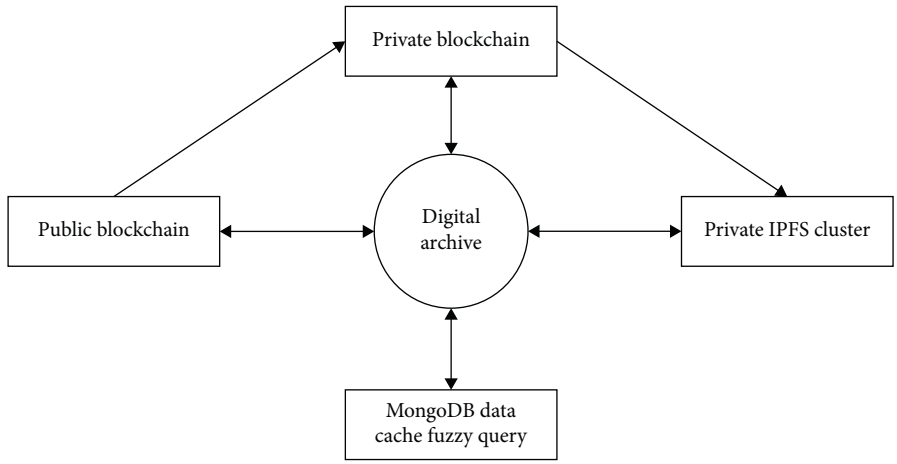

Figure 4: Blockchain data protection subsystem data storage scheme.

to store electronic files to realize the fuzzy query of the files. Private blockchains can control the speed of block packaging, obtain the benefits of generating blocks, and solve the problem of high data storage costs in public chains. When storing and dealing with limited amount of data, the relational databases such as MySQL perform well; however, when the data volume is large, it is hard for these relational database systems to handle the data. NoSQL, on the contrary, has the advantage to handle huge and unstructured data [22]. However, the private chain has shortcomings such as fewer nodes and poor security. Therefore, a combination of private chain and public chain is adopted to store archive information through the private chain, and the public chain is used to ensure the authenticity of the data on the private chain. IPFS has high data access efficiency and does not require payment, but its security and flexibility are not as good as blockchain technology. Therefore, a combination of blockchain and IPFS is adopted, and the private chain is used to call and protect file data in IPFS.

The content of the generated block in the blockchain cannot be tampered with; otherwise, it will not be accepted by other nodes; new blocks cannot be generated on this basis and therefore cannot be added to the main chain. To modify the data that has been written in the blockchain, the only way to replace the previous block with a new block is to use a fork, as shown in Figure 5. To modify the data of the block with a height of 1003, as a result, the hash value of all blocks after block 1003 changes. The public block chain uses the PCPC contract to access the block height and hash value of the private chain and realizes the protection of the file information on the private block chain.

4.3. Cost Analysis and Safety Assessment. Assuming that the number of intangible cultural heritage archive protection operations per month is α, the number of file modification operations is β, and the number of file borrowing operations is γ, the monthly cost of deploying all smart contracts on the public chain is $\text{Cost}_{\text{ethereum}}$:

$$\text{Cost}_{\text{ethereum}} = \alpha * \text{Cost}_{\text{protection}} + \beta * \text{Cost}_{\text{updateLog}} + \gamma * \text{Cost}_{\text{borrowLog}}. \quad (1)$$

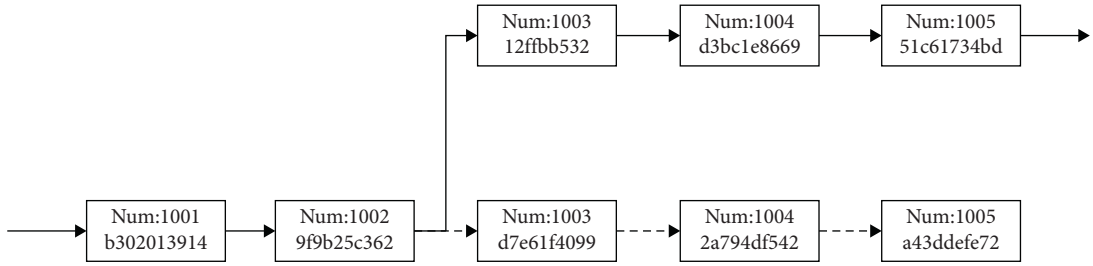

Figure 5: Blockchain bifurcation diagram.

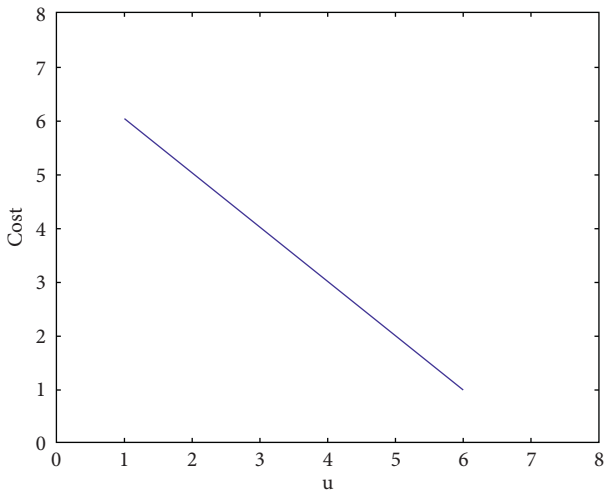

Figure 6: Relationship between u and cost.

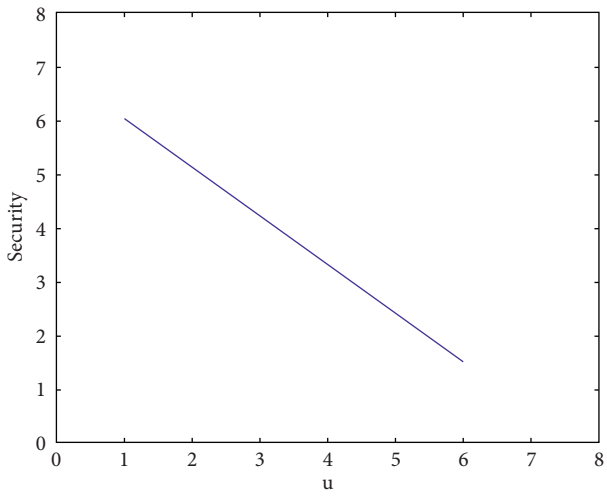

Figure 7: Relationship between u and security.

The combination of public and private chains deploys most smart contracts in private blockchain. Archives can continuously obtain digital currency in the private chain by creating blocks to pay for the transaction costs of smart contract calls. Assuming that the monthly operating cost of the private chain is w, every data storage operation of the smart contract will be recorded by the counter. When the counter can divide u, the public chain contract will be called to store the current block information in the private chain. The greater the value of the u parameter, the lower the economic cost of the solution and the greater the block height interval stored in the PCPC contract, and the protection of the private blockchain and the degree of data recovery will also decrease which is shown in Figures 6 and 7.

In the data-driven layer, public chain, private chain, private IPFS cluster, and database technology are comprehensively used to realize the protection, verification, and restoration of low-cost and high-efficiency electronic archives. In the system application layer, a RESTful interface service is designed by comprehensively using asymmetric encryption and digital signature technology, which can effectively prevent network attacks such as data theft and data tampering and achieve safe and reliable data communication between the system and the file management subsystem.

5. Conclusion

At present, the development of intangible cultural heritage management systems at home and abroad has been relatively mature, but the existing digital intangible cultural heritage management systems cannot solve the problem of data tampering from inside and outside the system in a better way. Therefore, the security and stability of the intangible cultural heritage management system and its protection against any kind of malicious attacks and intrusions have become the focus of attention in this field. After fully investigating the relevant materials of intangible cultural heritage management systems and blockchain technology, this paper proposes a plan to protect intangible cultural heritage through blockchain technology. The main contributions of this research work are the following:

(1) We designed and implemented a RESTful server and provided a data interaction interface for the users. We designed and implemented a blockchain data management platform, providing users with an intuitive and convenient way to query and view intangible cultural heritage data on the blockchain.

(2) Based on the Zabbix framework, a system monitoring platform was designed and developed. The platform is divided into four modules including server status monitoring, application error monitoring, stability assurance, and alarm sending. The system and monitoring platforms provide stability guarantees, monitor the running status of the server

host and application programs, and perform alarm operations when the server is offline or the program is abnormal.

Cultural heritage protection is important as it gives us a sense of who we are and gives us an irrefutable connection to the past. Art saves culture through passing on tradition and saves language, music, and craft. With the advancement in the information technology, it is important to think about using these technologies for the cultural heritage protection. In the future, we aim to develop a fully distributed system for the protection of intangible cultural heritage that would be capable of dealing with very large volumes of data using distributed data processing and storage technologies such as MapReduce and MapReduce-based frameworks.

Data Availability

The datasets used and analyzed during the current study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] F. Lenzerini, "Intangible cultural heritage: the living culture of peoples," *European Journal of International Law*, vol. 22, no. 1, pp. 101–120, 2011.

[2] M. Dragoni, S. Tonelli, and G. Moretti, "A knowledge management architecture for digital cultural heritage," *Journal on Computing and Cultural Heritage*, vol. 10, no. 3, pp. 1–18, 2017.

[3] P. He, G. Yu, Y. F. Zhang, and P. Constantinos, "Overview of blockchain technology and application prospects," *Computer Science*, vol. 44, no. 4, pp. 1–7, 2017.

[4] Huawei Technologies Co Ltd, *Huawei Blockchain White Paper [EB/OL]*, 2018.

[5] C. J. Dong, "The application of blockchain in the development prospects," *Information Technology and Standardization*, vol. 41, no. 12, pp. 12–15, 2017.

[6] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: a technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[7] S. Nakamoto, *Bitcoin: A Peer-To-Peer Electronic Cash System [EB/OL]*, https://bitcoin.org/bitcoin.pdf, 2008.

[8] CO. L. Poex, *What Is Proof of Existence? [EB/OL]*, pp. 04–29, 2018, https://poex.io/about.

[9] W. Li, Y. Chai, F. Khan et al., "A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system[J]," *Mobile Networks and Applications*, vol. 12, no. 5, pp. 1–19, 2021.

[10] J. B. Wayne Vaughan, *What Is a Chainpoint Proof? [EB/OL]*, pp. 04–29, 2018.

[11] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Proceedings of the A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology*, pp. 369–378, Springer-Verlag, San Jose, CA, 1987.

[12] A. Azaria, A. Ekblaw, T. Vieira, and L. Andrew, "MedRec: using blockchain for medical data access and permission management," in *Proceedings of the International Conference on Open and Big Data*, pp. 25–30, IEEE, Vienna, Austria, May 2016.

[13] Xinhuanet, *Alipay's Charity Donation Platform Fully Introduces Blockchain Technology to Create Transparent Public Welfare [EB/OL]*, pp. 12–21, 2016.

[14] J. Li, J. Cai, F. Khan et al., "A secured framework for SDN-based edge computing in IoT-enabled healthcare system," *IEEE Access*, vol. 8, no. 15, pp. 135479–135490, 2020.

[15] H. Zhao, *Intelligent Health Promotion Service System for Exercise Intervention for Chronic diseases*, University of Science and Technology of China, China, 2016.

[16] R. Olups, *Zabbix Network Monitoring*, Packt Publishing Ltd, Mumbai, India, 2016.

[17] M. Pilkington, "Blockchain technology: principles and applications," *Social Science Electronic Publishing*, vol. 32, no. 12, pp. 212–311, 2016.

[18] X. Y. Xia, *Design and Implementation of Blockchain-Based Equity Asset Purchase and Transfer*, Inner Mongolia University, China, 2016.

[19] C. Győrödi, R. Győrödi, G. Pecherle, and A. Olah, "A comparative study: MongoDB vs. MySQL," in *Proceedings of the 2015 13th International Conference on Engineering of Modern Electric Systems (EMES)*, pp. 1–6, IEEE, Oradea, Romania, June 2015.

[20] Q. Xia, F. J. Zhang, and C. Zuo, "Summary of the consensus mechanism of encrypted digital currency system[J]," *Computer System Application*, vol. 26, no. 4, pp. 1–8, 2017.

[21] M. A. Jan, F. Khan, R. Khan et al., "Lightweight mutual authentication and privacy-preservation scheme for intelligent wearable devices in industrial-CPS," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5829–5839, 2020.

[22] M. H. Zhao, L. Zhang, and J. Qian, "The trusted service management framework of social Internet of things based on blockchain," *Telecommunications Science*, vol. 13, no. 10, pp. 19–25, 2017.