Hindawi
Advances in Multimedia
Volume 2022, Article ID 4578525, 8 pages
https://doi.org/10.1155/2022/4578525

Research Article

Design and Implementation of a Data Sharing Model for Improving Blockchain Technology

Xiaowei Wang

Information Management Center, Physical Education College of Zhengzhou University, Zhengzhou 450052, China

Correspondence should be addressed to Xiaowei Wang; wxiaowei@peczzu.edu.cn

Received 11 March 2022; Revised 20 April 2022; Accepted 3 May 2022; Published 19 May 2022

Academic Editor: Qiangyi Li

With the continuous development of technology, the advancement of various data sharing technologies has gradually penetrated into various fields. Thus, data sharing and security are vital to realizing the value of the data. Nevertheless, the original data sharing model is not easily monitored for traces of electronic data use. In addition, the reluctance of data providers to share their data is also a problem. In order to address the issues of traditional centralized data sharing and management in terms of security and control, this research proposes the data sharing model based on blockchain technology, thereby enabling secure access to data. Furthermore, this study evaluates the model in terms of functionality and security. The results show that the blockchain-based data sharing model designed in this paper has great feasibility, security, controllability, and efficiency.

1. Introduction

In recent years, with the continuous development of the Internet and big data technology, data have played an irreplaceable role in people's social life and scientific research, and data sharing and distribution has gradually become an important means to promote social and scientific development. Secure data sharing is an important part of promoting the implementation of national big data strategies. The convergence of information in today's society has led to a huge amount of resources reaching into production and life at the same time, bringing huge changes to the society. Various industries are using big data to create huge social and economic value, such as medical data [1–3], financial data [4–6], energy data [7–11], and weather data [12, 13]. However, while the development of big data technology has brought convenience to people, it has also given rise to a number of issues in terms of data security. One of the severe issues is the frequent occurrence of security incidents such as security boundaries of data management and resource theft. The formation of resource barriers due to data security, privacy issues, and commercial factors makes it difficult to tap into the value of data, and the economic benefits of cross-referencing various types of data do not reach the full potential they contain. At the same time, due to technical limitations, most existing data sharing systems are unable to ensure data security. The traditional data sharing system uses centralized servers and centralized storage, which has many drawbacks. Firstly, with centralized management, administrators have a high level of authority, which can lead to data leakage from within. In addition, centralized servers are prone to hacking, causing a single point of failure, and once the server is down, the whole system will no longer be available. Furthermore, there is a risk that the centralized service may be terminated due to poor operations, which would result in the loss of all user data and no guarantee of data security. In conclusion, under the traditional data sharing system, users have no choice but to trust a third-party platform, which is extremely unsafe and unsecured.

Most traditional data sharing technologies use offline transmission in order to adequately ensure data security. The disadvantage of this is that it is not very real time and can easily cause serious problems such as data loss. In recent years, with the continuous development of the Internet and technology, online data sharing has become the main method of data transmission. Compared to offline transmission methods, online data transmission has obvious advantages in terms of timeliness [14]. However, with the

explosion of data on the Internet, higher requirements will be placed on data security storage, data security sharing, and efficient data sharing means. Therefore, traditional data transmission technologies can hardly meet the modern requirements for data security and privacy. In this context, the decentralized, auditable, and tamper-proof features of blockchain itself make it an important technology to study for data sharing [15]. However, the simple combination of blockchain and data sharing cannot achieve the requirements for secure and efficient data sharing.

A large number of scholars have conducted some research on blockchain-based data sharing and data distribution and have provided some unique insights. Hu et al. proposed a distributed privacy-preserving search scheme based on Ethernet smart contracts that implements a search of encrypted data on a malicious server but does not consider fine-grained access control of the data [16]. Zhang and Lin constructed a blockchain-based electronic health data sharing scheme for the needs of electronic medical record sharing and designed both private and federated chain structures, but the use of searchable public key-based encryption and the existence of cross-chain behavior are not efficient in operation [17]. Su et al. developed a trusted data sharing platform with on-chain storage and off-chain transmission, i.e., the request and response records of the shared data are up-chained and the original data are for secure transmission [18]. This architecture can theoretically alleviate the problems of system overload and privacy protection to a certain extent. Qiu and Zhu proposed a two-chain structured infectious disease data sharing model, combined with IPFS storage, to solve the problem of blockchain big data storage, which can protect data privacy and security to a certain extent [19]. Dias et al. pointed out that personal health data can be shared in conjunction with blockchain, providing privacy protection and a reward system to ensure that personal data are made public while attracting users to share relevant data [20]. Nuss et al. proposed fine-grained access control in combination with blockchain to protect data privacy, with blockchain nodes performing permission checks and key management operations and using the interstellar file system for data content storage [21].

There are two important research directions for blockchain-based sharing research, secure data storage and data security management. In terms of secure data storage, Wang et al. used the blockchain technology to guarantee a data storage framework for peer-to-peer transaction transparency and security [22]. This framework adopts proof of storage to verify that the host is not interfering with the data in the blockchain, but the system does not encrypt or decrypt the data before uploading it to the storage component, threatening the confidentiality and privacy of user data. Zheng et al. combined cloud storage and blockchain technology to share health-related information in a secure and transparent manner, using cloud storage to store data in an encrypted format and pointers to the location of the dataset to ensure the integrity of the dataset [23]. In the area of data security management, Bera et al. designed a blockchain technology-based approach to resource access control that combines the Scalable Access Control Markup Language standard for attribute-based access control with blockchain and implements the deployment of its rules in Bitcoin systems [24]. Xu et al. proposed a decentralized access control mechanism that combines a ciphertext policy attribute-based encryption algorithm with a blockchain to verify the legitimacy of a user's access privileges [25]. Li et al. combined blockchain and decentralized attribute ciphertext encryption algorithms for user privacy protection, embedding algorithm-related information in blockchain transactions and using blockchain nodes for related algorithm execution for user privacy protection [26]. This approach to privacy protection is better for attribute management, as it decentralizes the rights of a single attribute authority while placing attribute management in the hands of a professional attribute authority, effectively avoiding a situation where a single authority has too much power and triggers illegal authorization. However, this solution is limited by the way in which attribute-related information is passed through transaction information and does not allow for dynamic determination of environmental attributes at the time of user request. Qian et al. developed a security management model based on the blockchain technology for various IoT devices throughout their lifecycle. Mehedi et al. used terminal devices as networking technologies, combined with blockchain platforms, to produce backends that ensure high availability, security, and privacy while replacing traditional backend systems.

In conclusion, based on the existing research conducted on data sharing in blockchain, the main problems are that the centralized storage as supplementary storage has the disadvantages of non-scalability, weak disaster tolerance, and high personal maintenance cost due to the limited storage capacity of blockchain. Besides, there is a lack of confidentiality protection for the data uploaded to the blockchain supplementary storage. On the other hand, the shared security access to data can be realised through access control, but it is lack of protection of confidentiality of the data itself. Therefore, in order to solve the security problems of the traditional data sharing system, this study proposes a blockchain-based data security sharing model, which discards the traditional data sharing model based on centralized servers.

2. Data Sharing and Blockchain Technology

2.1. Blockchain Technology. The essence of blockchain technology is a distributed shared database, whose data structure is a chain structure. The block data structure is shown in Figure 1. Actually, each block is divided into block head and block body, and blocks are formed by hash pointers in series with each other.

The implementation of blockchain public ledger is based on cryptography, distributed consistent protocol, peer-to-peer network, smart contract, and other technologies, which are decentralized, tamper-proof, traceable, and transparent. It is decentralized, traceable, and open and transparent. Combining blockchain technology with data sharing and distribution can effectively solve the drawbacks of centralized data sharing such as single point of failure that commonly exists, and it has a broad application prospect.

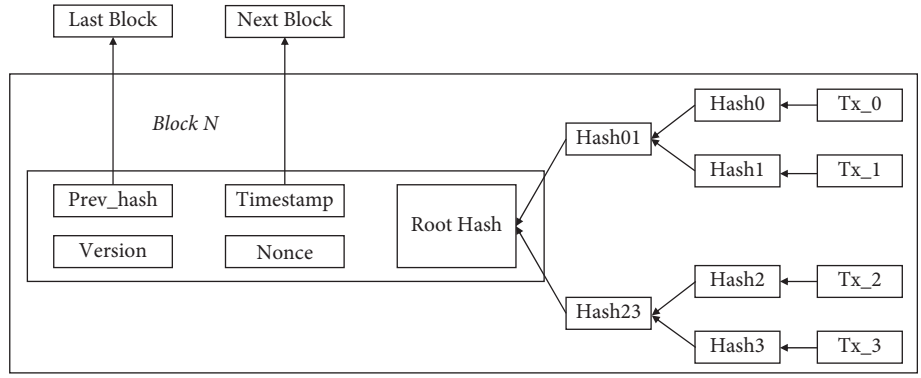

Figure 1: Block data structure.

Nowadays, there are three main types of blockchains: public chains, private chains, and coalition chains. Public chains belong to a blockchain composed of public participation, which are decentralized and do not contain a single entity to control the network. However, in some blockchain application scenarios, it is not expected that all users of the system will have equal access to all data, and the blockchain structure where authenticated nodes are allowed to participate and access data is private chain. Many companies establish private chains that are partially decentralized, only a small number of nodes are selected to achieve consensus, and most of the power on the private chain is assigned to individuals. Thus, the permission chain is a type of blockchain where management is centralized within the blockchain. Coalition chains are proposed to eliminate the drawbacks of private chain and are considered a kind of blockchain in the middle of public and private chains. Coalition chains allow specific organizations and nodes to participate in consensus and are partially decentralized compared to the centralized network of private chains, where a part of the organization that chooses to join determines the consensus.

The three different types of blockchain message pairs are shown in Table 1. In terms of reaching consensus, all nodes of a public chain participate in consensus, and the consensus of an organization's private chain is determined internally by its organization, while a coalition chain is responsible for consensus through a specific set of nodes. In terms of block information reading permission, public chains can openly view transaction information, while private chains and coalition chains can choose to restrict or open permission according to their actual application needs. In terms of efficiency, due to the large number of nodes in the public chain and the many nodes involved in consensus, it takes longer time to publish transactions and blocks, while private chains and coalition chains have limited data of participants into blocks with higher efficiency.

2.2. Interplanetary File System. Interplanetary File System (IPFS) is an open-source distributed file system. Unlike traditional centralized file systems that can only rely on servers to download files, IPFS runs on a P2P network, avoiding the single point of failure and vulnerability to attacks that traditional centralized networks are prone to. At the same time, as files are transferred from user to user, there is no speed limit of the central server, which greatly improves the efficiency of file transfer. In addition, since the traditional location-based addressing method can easily cause loss of resources, IPFS defines a distribution protocol based on content addressing. Each file has a unique hash value corresponding to it, which is not only tamper-proof but also prevents uploading large amounts of duplicate data and improves network efficiency. In conclusion, IPFS has several main advantages. Firstly, IPFS has the advantage of being decentralized and fast. Specifically, all data on IPFS are stored on the user's own computer and other users can retrieve data from the nearest IPFS user node. In addition, IPFS can be integrated better with blockchain. It can make up for the shortcomings of the blockchain's distributed ledger storage capacity by enabling a junction portal between high-capacity data and the blockchain by writing to the blockchain with an IPFS link to the data.

2.3. Searchable Encryption Technology. Searchable encryption technology allows the search process of encrypted data without revealing any information to the untrusted server. Specifically, (1) the untrusted server cannot obtain any information about the plaintext through the ciphertext only; (2) the untrusted server can search only under the authentication of the legitimate user; (3) the user does not have to indicate the specific meaning of the keyword when initiating a search request to the server; (4) the untrusted server cannot obtain any information about the query results in plaintext. Searchable encryption enables the server to return ciphertext files based on legitimate users' query requests while not being able to obtain users' personal private data, which ensures the security and privacy of users' data without unduly reducing the query efficiency.

3. Data Sharing Model Based on Blockchain

3.1. Blockchain-Based Secure Data Storage. The subjects of the data sharing process include data owners and data requesters, and the direction of data transfer is from data owners to data requesters. In order to realize the secure

Table 1: Comparison of different blockchains.

Type	Consensus	Reading permission	Efficiency
Public chain	All nodes reach consensus	Open access for all	Less efficient
Private chain	Some nodes within an organization reach consensus	Open permissions within an organization	Highly efficient
Coalition chain	Selected partial nodes reach consensus	Restricted permissions	Highly efficient

storage of data and the association between on-chain data and off-chain data, this study adopts blockchain, smart contracts, IPFS, and other technologies. The two important processes of data secure sharing process are data owner uploading resources and data requester requesting resources. The details of data sharing from data owner to data requestor are described as follows.

3.1.1. Data Upload Phase. The data owner first selects the data it wants to share, generates the symmetric key K to encrypt the data, and then obtains the encrypted information EI. The data owner constructs the licensed policy tree T and encrypts the symmetric key using the attribute permission public key and system parameters. Equations (1) and (2) can represent this process.

$$\text{Encrypt Data}(I, K) \longrightarrow EI, \tag{1}$$

$$\text{Auth Encrypt}(T, K) \longrightarrow EI. \tag{2}$$

3.1.2. Data Request Phase. The data requester first performs data retrieval, invoking the data list acquisition and data retrieval methods in the data management contract to determine the target data. Then, the encrypted information EI can be obtained. After that, the data requester can request the user key UK from the institution X to obtain the symmetric key K. This process can be expressed by equations (3) and (4).

$$\text{Decrypt}(UK, CI) \longrightarrow K, \tag{3}$$

$$\text{Decrypt Data}(CI, K) \longrightarrow I. \tag{4}$$

3.2. Blockchain-Based Access Control. In order to realize the secure transfer of symmetric keys and data information in the blockchain-based distributed data security access model, this study proposes a blockchain-based fine-grained dynamic access control model for this model based on the results of requirement analysis. The specific process is as follows.

3.2.1. Initialization Phase. As shown in equation (5), in the early stages of system building, the N th order bilinear group D needs to be constructed.

$$N = m_1 \times m_2 \times m_3, \tag{5}$$

where m_1, m_2, m_3 are prime numbers.

Then, the generated unit d of D's subgroup D_s can be derived. At the initialization phase, the authorization authority X calls the authorization initialization method to select two random indices α_i and β_i for each attribute i in the attribute set G. With public parameter P and attribute space G as input, the permission key SK and the permission public key PK are obtained. This process can be expressed as

$$(SK, PK) = \text{Authority Key Gen}(G). \tag{6}$$

3.2.2. Controlled Request Phase. Dynamic attributes at refer to information that changes with time or the location of the data requester such as the current access timestamp, the current Internet Protocol address of the controlled requester, and other dynamic information. AT can be expressed as

$$AT = \{at_1, at_1, \ldots, at_n\}. \tag{7}$$

3.2.3. Data Decryption Phase. The controlled requester can obtain the key and related information if it has been determined by the data request authority. The decryption algorithm is first performed locally to obtain the user system key K. The controlled requester performs the decryption algorithm to decrypt the encrypted information EI with the user key K.

3.3. Blockchain-Based Data Sharing Technology. The blockchain-based distributed data security sharing solution can be divided into two modules according to its function, the access control module and the data management module. The solution is divided into three key implementation layers, from top down, the user access layer, the blockchain engine layer, and the data storage layer, as shown in Figure 2.

The user access layer is the user-oriented operational layer that provides the logical implementation of the main functions of the model. This layer is the logical implementation module corresponding to the functional modules of the data sharing model, the same access control module, and the data management module. These three logical implementation modules will accept the information provided by the blockchain engine layer and data storage layer to interact with the user to achieve logical access control and data management-related functions. The blockchain engine layer is the backend implementation support layer for the user access layer. The blockchain plays a vital role in the data sharing model as an important storage and operational auditing engine for system information. The data storage layer is the user data storage layer, providing secure storage for shared data. To ensure the security of data storage, the storage method is confirmed as IPFS storage.

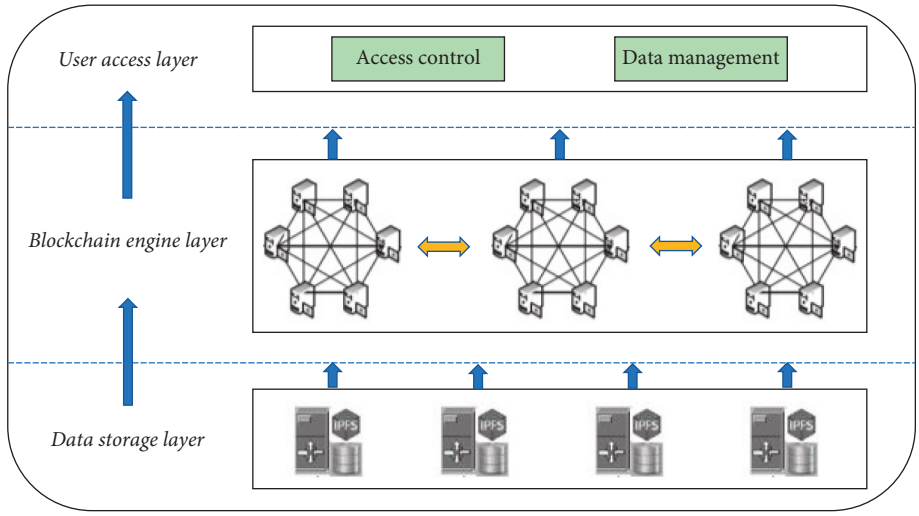

Figure 2: Framework of blockchain-based data sharing model.

3.3.1. Access Control Module. The framework of the access control module is shown in Figure 3.

The functions required by the access control module are divided into three subfunctions, identity management, attribute management, and encryption and decryption. The target information decryption and ciphertext decryption of the encryption and decryption module do not involve blockchain-related storage and auditing, so the specific implementation is done at the user access layer. The identity management, attribute management and information storage functions, and attribute query functions of the encryption and decryption module are concluded in the operational auditing or blockchain storage, so the logical interface is implemented in the user access layer and the blockchain layer performs the functional implementation.

3.3.2. Data Management Module. The functions required for the data management module are abstracted into the following three modules: data information management module, data storage module, and encryption and decryption module (Figure 4). The data content itself is stored in the data access layer by IPFS, while the data meta-information is stored in the blockchain by the blockchain engine layer for maintenance and query of data information.

3.4. Data Sharing Blockchain Engine. The data sharing blockchain engine can implement customized functionality by writing smart contracts. The blockchain engine designed in this study follows a variety of software design principles, using layered, modular design principles to ensure that the system logic is clear and easy to present while developing the interface and returns values for this solution for data sharing operations. In addition, the blockchain itself meets the requirements of the rules for security and auditability. The data sharing blockchain engine can be divided into three layers according to its function: the interface layer, the core layer, and the storage layer. Each of the large functional layers of the engine contains its own internal smaller functional modules. The blockchain engine architecture is shown in Figure 5.

3.5. Hardware and Software Environment for Model Development. The hardware environment for the data sharing model based on blockchain technology is shown in Table 2.

On the other hand, the software environment for the data sharing model based on blockchain technology is shown in Table 3.

4. Evaluation of Data Sharing Model Based on Blockchain

In order to verify the feasibility of the data sharing model based on blockchain, this research will analyze and evaluate in terms of functionality and security.

4.1. Functionality Evaluation. In the data sharing model designed for this study, identity management of data users is implemented, using CP-ABE for fine-grained access control, with the data owner assigning administrative unique numbers and attribute information to registered users. By distinguishing between dynamic and static attributes and configuring different access control policies for each of the two different states of attributes, dynamic access rights determination is achieved in stages while supporting dynamic update of access policies. At the same time, smart contracts are used as the entrance and route to change the state of the blockchain, and the programmable effect facilitates the provision of interfaces for users to retrieve data on the chain by keywords to obtain lists or queries.

4.2. Security Evaluation. Compared to traditional data sharing schemes, the model proposed in this study makes extensive use of the concept of decentralization, thus effectively avoiding the problem of single point of failure. Firstly, the overall design of this data sharing model is based on

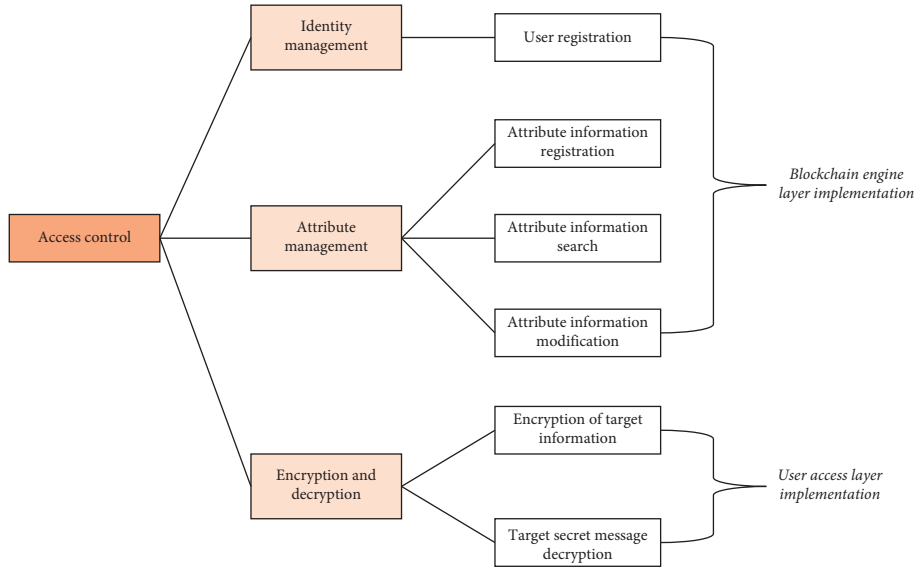

Figure 3: Framework of access control module.

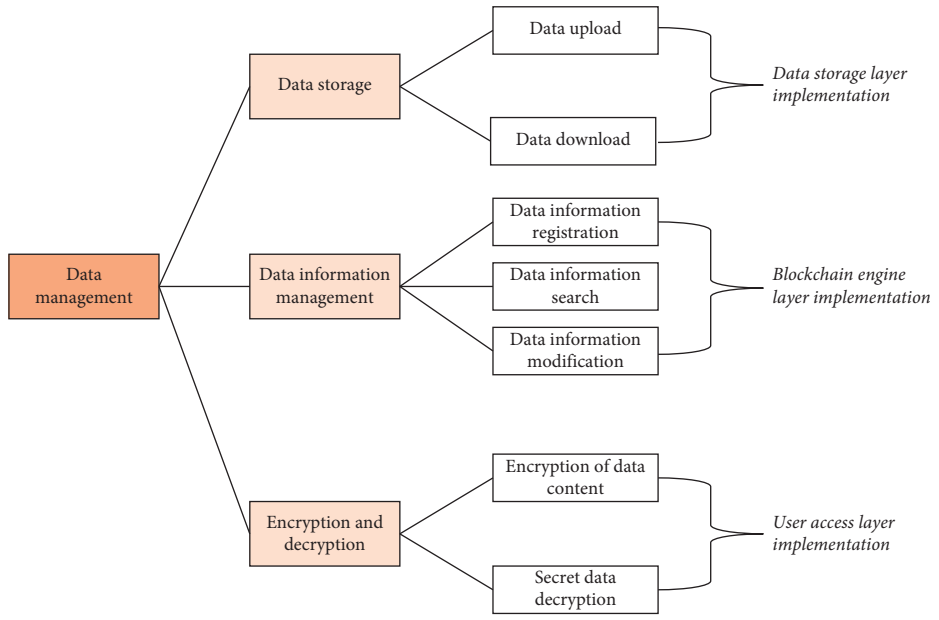

Figure 4: Framework of data management module.

blockchain technology and IPFS storage devices. The decentralized and distributed nature of blockchain and IPFS itself ensures that even if some nodes fail, the scheme will not affect the overall availability of the scheme. Secondly, this model supports multiple attribute agencies for attribute management. The decentralization of attribute management power effectively controls the potential for illegal operations caused by centralized power and prevents the failure of a single attribute authority from blocking the solution's functionality. In addition, in contrast to the scenario where the data owner performs the attribute management, this research separates the attribute management from the data owner. The data owner only assumes the role of data manager and does not perform other user-managed operations, effectively avoiding the problem of data unavailability due to the data owner's failure to respond in a timely manner.

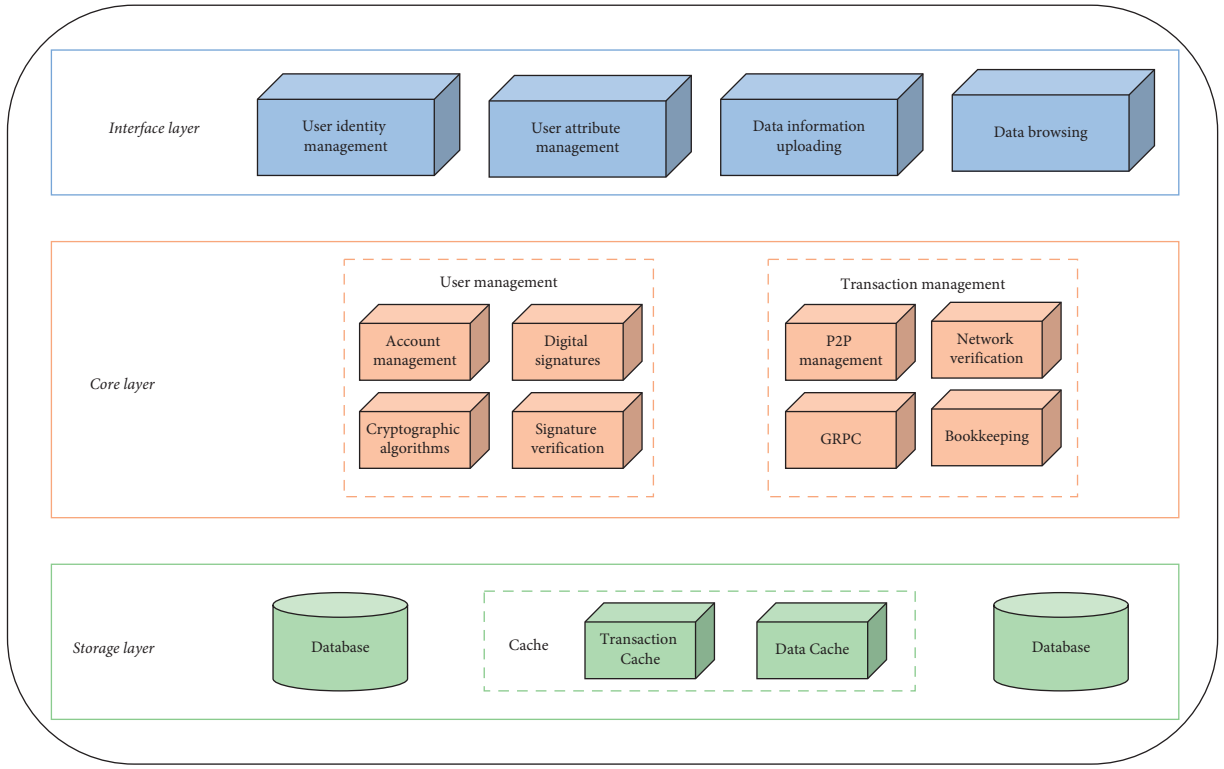

Figure 5: Data sharing blockchain engine.

Table 2: Hardware environment for the data sharing model.

Name	Data
Processor	Intel® Core™ i5-8300H CPU @ 2.30 GHz
Memory	8 GB
Operating system	Windows 10, Tomcat 9

Table 3: Software environment for the data sharing model.

Name	Data
Development tool	IntelliJ IDEA 2020.3
Virtual machine	Oracle VM virtualbox 6.1.3
Database	MySQL

5. Conclusion

Traditional data sharing has mostly been done offline to ensure data security, but it is prone to problems such as poor real-time performance and data loss. With the continuous development of Internet technology, online data sharing has become the main method of data transmission, which has obvious advantages over offline transmission methods in terms of timeliness. However, the explosion of Internet data in recent years has likewise put forward higher requirements for data regulation and privacy protection. Blockchain is a technology that combines cryptography, networking, distributed storage, and other technologies, and its own features such as decentralization and immutability of information on the chain can natively solve some of the problems of data sharing. In this context, this study investigates and applies blockchain-based distributed data security sharing technology.

This paper first proposes a blockchain-based data sharing model based on the current status of research on blockchain-based data security sharing at home and abroad. This model is based on the distributed fine-grained access control model of blockchain and the distributed data security access model based on blockchain, and there is a symmetric encryption of data content which can avoid data content leakage and act as the connection of the overall architecture. The underlying IPFS system is used as distributed storage, which can solve problems such as centralized storage single point of failure.

In the future, this research can be extended in the following ways. Firstly, the data sharing model proposed in this study can be optimized, attempting to introduce mechanisms such as theft tracking from the optimization algorithm itself and combining it with the data sharing scheme to make it more functional. In addition, the design and implementation of the storage layer can be optimized to improve the performance of the transmission by attempting to delineate the LAN and WAN modules according to different application scenarios.

Data Availability

The labeled datasets used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

Acknowledgments

This study was supported by the Scientific and Technological Project in Henan Province (Research on Construction and Application of the Remote Support Platform for Winter Sports Medicine and Rehabilitation Based on Blockchain) (nos. 202102310323 and 212102310264).

References

[1] W. N. Price and I. G. Cohen, "Privacy in the age of medical big data," *Nature Medicine*, vol. 25, no. 1, pp. 37–43, 2019.

[2] Q. Yao, Y. Tian, P.-F. Li, L.-L. Tian, Y.-M. Qian, and J.-S. Li, "Design and development of a medical big data processing system based on Hadoop," *Journal of Medical Systems*, vol. 39, no. 3, pp. 23–11, 2015.

[3] A. T. Azar and A. E. Hassanien, "Dimensionality reduction of medical big data using neural-fuzzy classifier," *Soft Computing*, vol. 19, no. 4, pp. 1115–1127, 2015.

[4] M. Cao, R. Chychyla, and T. Stewart, "Big data analytics in financial statement audits," *Accounting Horizons*, vol. 29, no. 2, pp. 423–429, 2015.

[5] P. Cerchiello and P. Giudici, "Big data analysis for financial risk management," *Journal of Big Data*, vol. 3, no. 1, pp. 18–12, 2016.

[6] W. Wang, W. Li, N. Zhang, and K. Liu, "Portfolio formation with preselection using deep learning from long-term financial data," *Expert Systems with Applications*, vol. 143, Article ID 113042, 2020.

[7] B. Cheng, K. Lu, J. Li, H. Chen, X. Luo, and M. Shafique, "Comprehensive assessment of embodied environmental impacts of buildings using normalized environmental impact factors," *Journal of Cleaner Production*, vol. 334, Article ID 130083, 2022.

[8] C. Zhang, L. Cao, and A. Romagnoli, "On the feature engineering of building energy data mining," *Sustainable Cities and Society*, vol. 39, pp. 508–518, 2018.

[9] J. P. Gouveia, J. Seixas, and G. Long, "Mining households' energy data to disclose fuel poverty: lessons for Southern Europe," *Journal of Cleaner Production*, vol. 178, pp. 534–550, 2018.

[10] K. Amasyali and N. M. El-Gohary, "A review of data-driven building energy consumption prediction studies," *Renewable and Sustainable Energy Reviews*, vol. 81, pp. 1192–1205, 2018.

[11] R. Yuan, F. Guo, Y. Qian et al., "A system dynamic model for simulating the potential of prefabrication on construction waste reduction," *Environmental Science and Pollution Research*, vol. 29, no. 9, pp. 12589–12600, 2022.

[12] Y. Qian, S. Chen, J. Li et al., "A decision-making model using machine learning for improving dispatching efficiency in chengdu shuangliu airport," *Complexity*, vol. 2020, Article ID 6626937, 2020.

[13] A. Moazami, V. M. Nik, S. Carlucci, and S. Geving, "Impacts of future weather data typology on building energy performance - investigating long-term patterns of climate change and extreme weather conditions," *Applied Energy*, vol. 238, pp. 696–720, 2019.

[14] S. Q. Dai, H. Li, J. Xiong et al., "Assessing the extent and impact of online data sharing in eddy covariance flux research," *Journal of Geophysical Research: Biogeosciences*, vol. 123, no. 1, pp. 129–137, 2018.

[15] A. Zwitter and J. Hazenberg, "Decentralized network governance: blockchain technology and the future of regulation," *Frontiers in Blockchain*, vol. 3, p. 12, 2020.

[16] S. Hu, C. Cai, Q. Wang, C. Wang, X. Luo, and K. Ren, "Searching an encrypted cloud meets blockchain: a decentralized, reliable and fair realization," in *Proceedings of the IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, pp. 792–800, IEEE, Honolulu, HI, USA, April 2018.

[17] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *Journal of Medical Systems*, vol. 42, no. 8, pp. 140–218, 2018.

[18] Z. Su, Y. Wang, Q. Xu, and N. Zhang, "LVBS: lightweight vehicular blockchain for secure data sharing in disaster rescue," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, 2020.

[19] Z. Qiu and Y. Zhu, "A Novel structure of blockchain applied in vaccine quality control: double-chain structured blockchain system for vaccine anticounterfeiting and traceability," *Journal of Healthcare Engineering*, vol. 2021, pp. 1–10, Article ID 6660102, 2021.

[20] J. P. Dias, H. Sereno Ferreira, and Â. Martins, "A blockchain-based scheme for access control in e-health scenarios," in *International Conference on Soft Computing and Pattern Recognition*, pp. 238–247, Springer, Cham, December 2018.

[21] M. Nuss, A. Puchta, and M. Kunz, "Towards blockchain-based identity and access management for internet of things in enterprises," *Trust, Privacy and Security in Digital Business*, Springer, vol. 11033, pp. 167–181, 2018.

[22] S. Wang, X. Wang, and Y. Zhang, "A secure cloud storage framework with access control based on blockchain," *IEEE Access*, vol. 7, pp. 112713–112725, 2019.

[23] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, "Blockchain-based personal health data sharing system using cloud storage," in *Proceedings of the 2018 IEEE 20th International Conference on E-health Networking, Applications and Services*, pp. 1–6, Ostrava, Czech Republic, September 2018.

[24] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment," *Computer Communications*, vol. 153, pp. 229–249, 2020.

[25] R. Xu, Y. Chen, E. Blasch, and G. Chen, "Blendcac: a smart contract enabled decentralized capability-based access control mechanism for the iot," *Computers*, vol. 7, no. 3, p. 39, 2018.

[26] G. Li and H. Sato, "A privacy-preserving and fully decentralized storage and sharing system on blockchain," in *Proceedings of the 2019 IEEE 43rd Annual Computer Software and Applications Conference*, pp. 694–699, IEEE, Milwaukee, WI, USA, July 2019.