Hindawi
Mathematical Problems in Engineering
Volume 2022, Article ID 5126326, 8 pages
https://doi.org/10.1155/2022/5126326

Research Article

Smart Mobile Information Systems on the Key Systems of Blockchain Privacy Protection

Xiaobo Wei

School of Business, Xijing University, Xi'an 710123, Shaanxi, China

Correspondence should be addressed to Xiaobo Wei; 20060041@xijing.edu.cn

Received 18 April 2022; Revised 25 May 2022; Accepted 6 June 2022; Published 25 June 2022

Academic Editor: Wei Liu

In the process of data collaboration, the data source copyright, equity boundaries, and other issues must be ensured to ensure the data owner's income rights. The data on the blockchain are transaction data. After the data are verified, they are added to the block by the node that has the right to keep accounts. Once the data are added to the blockchain, they cannot be deleted or changed, and only authorized query operations can be performed. The transaction records on the blockchain are completely public, and the fund transactions between accounts can reflect a lot of valuable information, especially some special accounts track the IP of transaction users through methods such as address reuse, taint analysis, and cluster analysis. At the same time, a credit contribution certification mechanism is established to ensure that the contributions are directly proportional to the rewards, and finally, a credit mechanism for data fraud is established. This paper mainly analyzes the key systems of privacy protection through research data and blockchain. The research results show that different companies conduct the Pailler homomorphic encryption of data and use the secure multiparty calculation to obtain the results. The execution of the whole process is controlled by a specific intelligent contract, and the records of the execution process are stored in the blockchain. It can be seen that the blockchain-based data distribution system changes the traditional data distribution mode so that the data source and the data user can interact directly, which promotes the maintenance of the system's security and stability.

1. Introduction

The data privacy of users in the cloud computing environment is secret data, which is information that others do not want to know. From the perspective of privacy owners, privacy data can be divided into personal privacy data and common privacy data. Personal privacy data include information that can be used to identify or locate individual and sensitive information. The privacy and accessibility of data can ensure the user's control over the information and make access to unrestricted information [1, 2]. The conflict between data privacy and accessibility occurs naturally [3, 4], and data in the urban traffic is closely related to these two characteristics [5, 6].

Big data has become China's national strategy. China needs to speed up. "Big data" requires new processing modes to have stronger decision-making power, insight discovery power, and process optimization ability to adapt massive, high growth rate and diversified information assets.

Each node has the same rights, and data updates and transaction validation are done through circulated hubs that follow an agreement system [7, 8]. Specifically, what is put away on the blockchain is not simply the exchange, yet the hash of the exchange [9, 10], which is stored in the form of Merkle trees in blocks that form chained data structures in chronological order and longest chain criteria [11]. Therefore, the construction of a unified, open, and diversified "chain network" blockchain infrastructure is important [12]. The important significance of building a blockchain framework is to ensure that data of different formats and sources can be integrated and that different applications can be perfectly integrated into the blockchain hotspot [13, 14].

2. Experimental Procedure

Blockchain is a distributed database technology developed on the basis of the application of digital encryption currency. The blockchain system has the characteristics of decentralization, immutability, distributed consensus, traceability, and eventual consistency, which makes it suitable for solving data management problems in untrusted environments. The unique data management function of blockchain has become the key to exerting the value of blockchain in applications in various fields. Blockchain technology is becoming more and more popular [15, 16]. Blockchain is a new type of distributed protocol, which can be realized without the mutual trust of nodes, thus effectively reducing the trust cost in the real economy [17, 18]. At present, the biggest application of blockchain technology is digital currency, and it is also one of the ten typical judicial technology applications of the Internet. Although blockchain significantly improves data security and reliability, the storage scalability of blockchain is poor [19, 20]. For example, bitcoin currently has a total capacity of more than 160 GB. The current bitcoin system uses nearly 1600 PB of storage space, only for about 160 GB of data, which greatly wastes storage space. In addition, as time goes by, the blockchain will increasingly occupy a large amount of node storage space. The function introduction of each part of the block header is shown in Table 1.

In this context, a scheme for implementing scalable is proposed and the extended blockchain storage is studied to realize the privacy protection of multiparty shared data:

$$c = E_{pk}(m) = g^m r^n \bmod n^2. \tag{1}$$

As shown in Figure 1, according to the homomorphic nature of the encryption system,

$$\begin{aligned} E_{pk}(m_1 + m_2) &= E_{pk}(m_1) + E_{pk}(m_2) \\ &= g^{m_1+m_2}(r_1 r_2)^n \bmod n^2, \\ E_{pk}(a \cdot m_1) &= E_{pk}(m_1)^a = g^{am_1} r_1^{an} m \bmod n^2, \\ C &= E_{pk}\left(\sum_{k=1}^{K} v_k\right) = \prod_{k=1}^{K} E_{pk}(v_k). \end{aligned} \tag{2}$$

The protocol presented in this study also supports partial anonymity. Imagine Alice wants to send some money to Bob, but he does not want anyone to know that these currencies are for Bob. Table 2 shows the roles assigned to users, the permissions each role has, and the relationship between user-role-permission-device.

Assuming n of account are chosen. Then, the $n-1$ address from the anonymous set is randomly selected. Finally, she performs the transfer, sending the ciphertext of the currency to a blind feature of $n-1$ addresses that are randomly selected.

In order to encrypt the message, an integer is randomly selected, and then, calculate the ciphertext:

$$E_{pk}(m, r) = (N+1)^m \cdot r^N \bmod N^2. \tag{3}$$

Table 1: The function introduction of each part of the block header.

Module	Size	Function
Version	4	Record the version number of the block header
Prev Block Hash	32	Record the hash worth of the past square
Merkle Root	32	Record the root value of the Merkle tree hash of the transaction contained in the current block
Timestamp	4	Record the creation timestamp of the current block
Difficulty Target	4	Record the computational difficulty of the current block
Nonce	4	Random number generated with the block

For decryption,

$$m = \frac{\left(E_{pk}(m, r)^{\lambda} \bmod N^2\right) - 1}{N} \cdot \lambda^{-1} \bmod N. \tag{4}$$

The given scheme can also use the consensus to recover the random number in a given ciphertext:

$$\begin{aligned} r &= c^{N-1 \bmod \lambda} \bmod N, \\ c &= E_{pk}(m, r) \cdot (N+1)^{-m} \bmod N. \end{aligned} \tag{5}$$

From the nature of the encryption system, the following equations can be obtained:

$$\begin{aligned} E_{pk}(m_1, r_1) \cdot E_{pk}(m_2, r_2) &= E_{pk}(m_1 + m_2, r_1 \cdot r_2), \\ E_{pk}(m, r)^k &= E_{pk}\left(k \cdot m, r^k\right). \end{aligned} \tag{6}$$

The Paillier encryption system also has a blind feature, which is the ability to change a ciphertext without changing the corresponding plaintext:

$$E_{pk}(m, r_1 \cdot r_2) = E_{pk}(m, r_1) \cdot E_{pk}(o, r_2). \tag{7}$$

Assuming different values (i.e., $x_m^{k_1} \neq x_m^{k_2}$), in the next place, in the payment privacy, if Alice is transferring money to n of accounts during the transfer, then only the probability of selecting Bob's account is $1/n$. The equipment information used in the mechanism simulation experiment in this paper is shown in Table 3.

By hiding each transaction with a different anonymous set, the rate of increase is gradually increased, as shown in Figure 2.

3. Results and Discussion

3.1. Blockchain-Based Enterprise Data Collaboration and Sharing Solution. The blockchain-based undertaking information cooperation and sharing plans are given in Figure 3. The main roles of the scheme are the homomorphic encryption scheme, the contribution proof protocol, and the smart contract technology. It solved the problems existing in the current contribution of enterprise data collaboration.

Multiple enterprises participating in the collaboration encrypt the data to be shared homomorphic output the

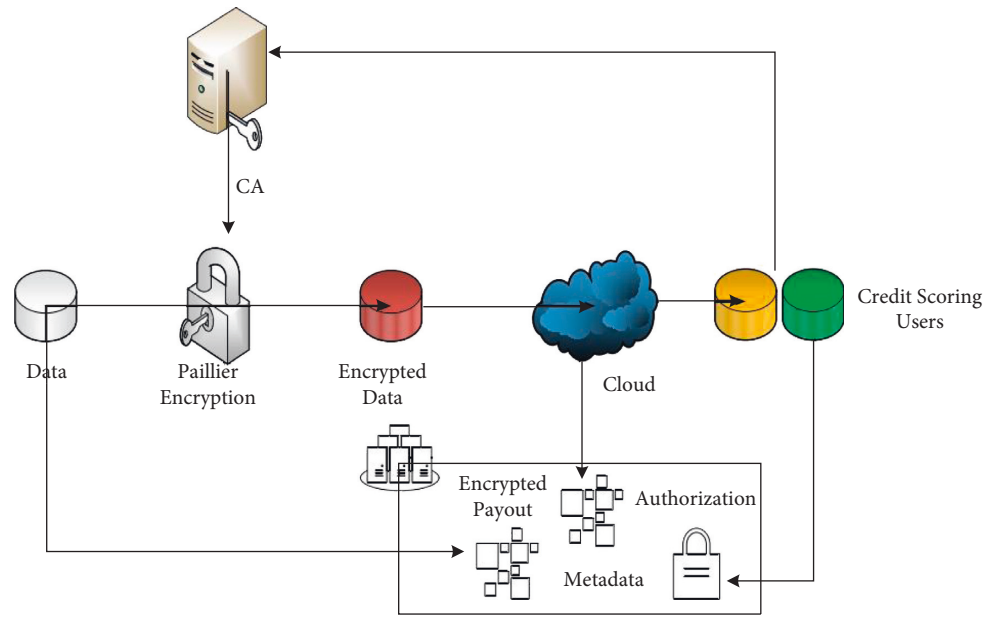

Figure 1: System model.

Table 2: Roles assigned to users, the permissions each role has, and the relationship between user-role-permission-device.

Module	Size	Function
Version	4	Record the version number of the block header
Prev Block Hash	32	Record the hash value of the previous block
Merkle Root	32	Record the root value of the Merkle tree hash of the transaction contained in the current block
Timestamp	4	Record the creation timestamp of the current block
Difficulty Target	4	Record the computational difficulty of the current block
Nonce	4	Random number generated with the block

Table 3: The equipment information used in the mechanism simulation experiment in this paper.

Equipment	CPU	Working	Memory (GB)	Hard disk
Lenovo Think Station P910	Intel Xeon E5-2640 v4, 2 4 GHz	Window 10(64 bit)	64	2 TB
Lenovo 10N9CTO1 WW	Intel Core i7-7700, 3.6 GHz	Window 7(64 bit)	8	2 TB
Lenovo N50	Intel Core i5-4210, 1.7 GHz	Window 7(64 bit)	4	500 GB
Raspberry model B	Contex A53, 1.2 GHz	Raspbian GNU/Linux 8	1	16 GB

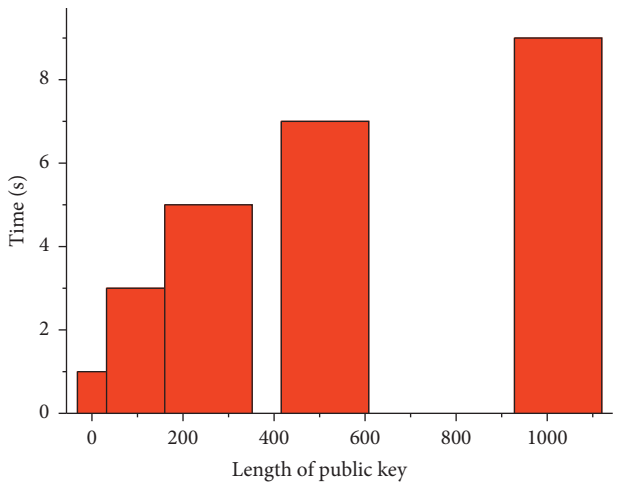

Figure 2: Paillier key generation time.

encrypted data, and use the secure multiparty computing technology to merge the previously designed algorithms together for collaborative computing. After the result of the safe multiparty calculation comes out, demander utilizes the Paillier homomorphic decoding calculation to unscramble the result and acquire the information that they really want. Each data provider and the collaborative data result calculation party distribute the predesigned total reward according to the score obtained, and under the control of another smart contract, the rewards that each party should receive are sent to the accounts of these users. Whatever the transmitted data, the process of data transfer, the process of collaborative data operations, the process of returning data results, the process of contributing proof calculations, the process of reward distribution, and the results are recorded in blockchain by smart contracts. This article records the results of multiple visits, as shown in Table 4.

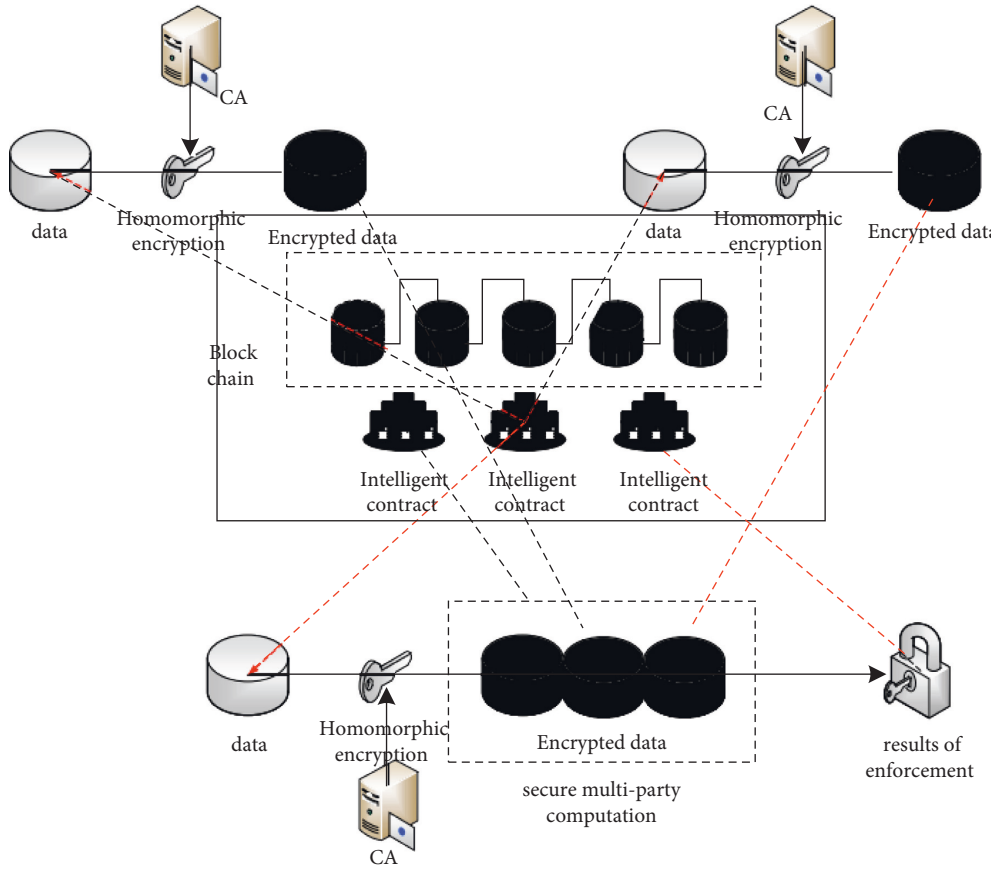

Figure 3: Execution process of enterprise data collaboration.

Table 4: Results of multiple visits.

User	Role	Operate	Results	Time
PK 1	Manager	Execute	Allow	2019.6.6 9:43
PK 2	Supervisor	Write	Allow	2019.6.6 15:35
PK 3	Partner	Storage	Deny	2019.6.7 10:15
PK 4	Client	Read	Allow	2019.6.7 15:42

3.2. Implementation Steps of Enterprise Data Collaboration and Sharing Based on Blockchain. Users participating in enterprise data sharing requirements, the data are prepared to be transmitted through the encrypted secure channel. It passes the data through a secret channel to a secure computing container. The relevant data are automatically encrypted, automatically decrypted, and ready to perform related operations, as shown in Figure 4.

Received data are manipulated using a secure multiparty computing algorithm that implements the determination, as shown in Figure 5.

Under the strong supervision through the reverse one-way secure channel, the collaborative data result is immediately eliminated after being delivered to the collaborative data requester and is not backed up, as shown in Figure 6.

Without leaving a backup, raw original is also done, as shown in Figure 7.

Due to the huge number of IoT devices, in order to satisfy as many access requests of IoT devices as possible, local

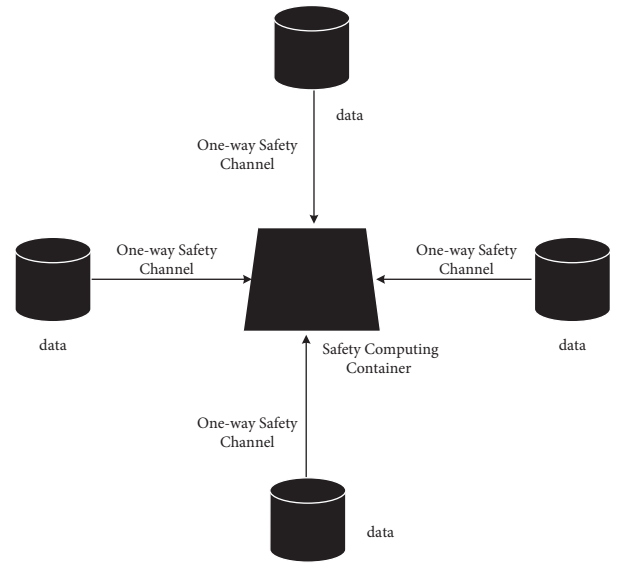

Figure 4: Collaborative data transmission.

gateways need high-performance features. Therefore, this article tried the throughput and data transmission of the neighborhood door, and the experimental outcomes are displayed in Figure 8.

The initiator information stored by the verification node is shown in Table 5.

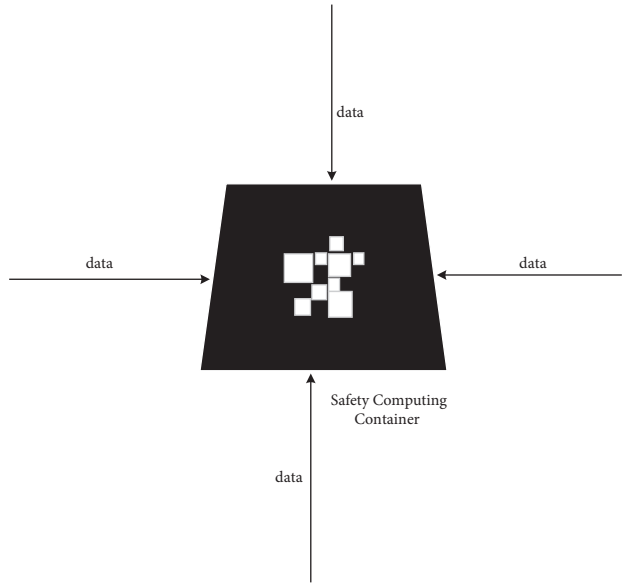

Figure 5: Collaborative data operation.

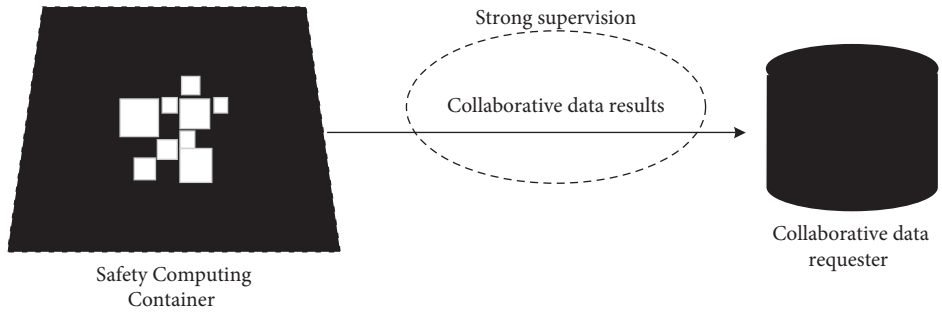

Figure 6: Collaboration data return.

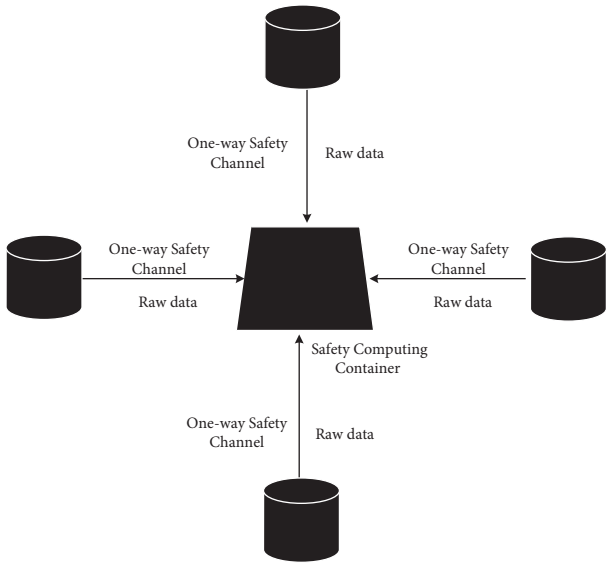

Figure 7: Raw data return.

Taking into account the network delays in real transactions, this experiment introduces network delays when simulating the transaction process, taking random numbers as 0.21587, 0.76817, 0.16967, 0.57892, 0.82071, 0.68045, 1.26064, 0.77601, 0.55335, and 0.34181. The transaction delay value of each round of simulation is displayed in Table 6.

Users with high permissions can check the statistics of these health data at any time through the authorized homomorphic public key. However, since the private key signature is added during cannot be spied on before the permission of the SP is obtained. User privacy data are shown in Table 7.

3.3. Blockchain-Based Government Data Collaboration and Sharing Solution. In this study, through the decentralized blockchain technology, an innovative data distribution system is constructed. Blockchain technology is mainly proposed for the trust problem of the centralized accounting system of existing financial institutions. It is composed of distributed storage, P2P network, encryption algorithm, consensus mechanism, and other technologies. In the system proposed in this study, there are six different roles, namely information source, media, information buyer, system maintainer, content distributor, and advertisers.

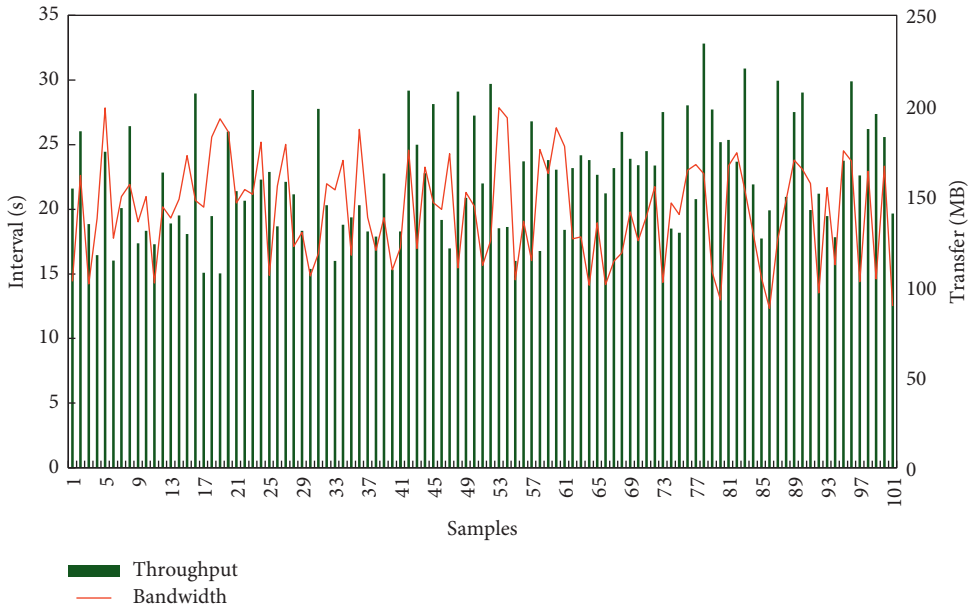

Figure 8: The test results.

Table 5: The initiator information stored by the verification node.

Rounds	Alice	Bill	Mark	Joan
Round1	354414	7.80769	6.92872	3.57067
Round2	6.86712	4.72692	5.68037	4.99165
Round3	0.37410	7 35849	6.30477	3.64614
Round4	4.43557	6.27414	5.70371	3.88766

Table 6: The transaction delay value of each round of simulation.

Numbers	Alice	Bill	Mark	Joan
1	254454	7.70725	2.52772	2.57027
2	2.72752	4.72252	5.27027	4.55525
3	0.27450	7 25745	2.20477	2.24254
4	4.42557	2.27454	5.70275	2.77722

Table 7: User privacy data.

Index	User ID			
	1	2	3	4
HR	88	76	90	77
BP	107	124	110	101
RR	16	13	18	12

The information source uploads the created information to a given blockchain system, while doing this, the information source needs to provide a certain commission to the system. The source of information generally refers to the information transmitted through a certain substance; that is, the origin/source of the information (including the place of production and occurrence of information resources, the source, and the base). The information source can use built-in smart contract module in the system to initiate content crowdfunding and set the revenue share portion and investment deadline for the transfer. Within the limited time, the information buyers can invest the content by share, and the content producer can obtain the lump sum basis at first, and the content will be automatically allocated in portions by the smart contract to the information source and the investor in information purchaser after the lock-up period. The media is the medium, in which information buyers contact information published by information sources, and is also the channel through which advertisers place advertisement [21, 22]. The media enjoys the advertising share in proportion to the prearranged smart contract, which encourages the media to expand the user base and improve the user experience. Information sources can be divided according to the storability of information, the time sequence of production, the form of existence, the production process, and the content of the generated information.

3.4. Research on Blockchain Data Distribution System. The data purchasers are require to pay a specific measure of cost to the data source and the fundamental asset supplier while buying the data in the framework. The information buyers can participate in the crowdfunding initiated by the information source; that is, the users are allowed to invest in the excellent content generated by other users and obtain the part of the revenue share, while the information buyers can also share the content, the sharing action is recorded by the smart contract on the blockchain, and profit share can be obtained from the advertising revenue of the shared content [23]. Framework maintainers come to a settlement on an agreement system to finish the information on the blockchain. System maintainers have high requirements for computing and communication resources. The main sources of revenue for system maintainers are consensus incentives and transaction fees charged.

Multimedia information dissemination and sharing have high requirements on the network, including storage and

streaming media forwarding cost, which can account for more than 40% of operating costs. In a blockchain-based information distribution system, users with idle resources and eco-partners can voluntarily join nodes to provide bandwidth and storage capacity services for blockchain-based information distribution system users and obtain corresponding commission incentives; thereby, the operating costs in the ecosystem have been significantly reduced. Advertisers are able to pay for advertising based on the data because the clicks, downloads, or page views of the content on the blockchain-based information distribution system are publicly transparent.

Information sources can upload, categorize, fill brief introduction, and fix a price of their own work. Consumers can search the platform for their favorite content and authors, browse content by category, view content profiles and user reviews, purchase content, and rate and comment on purchased content.

Considering that the blockchain-based data distribution system needs to store a lot of photos, videos, texts, and other information. The nodes in the blockchain-based data distribution system are divided into data storage nodes, system maintenance nodes, and common nodes. The data storage nodes are used to maintain the system's data resources. According to the incentive model of the blockchain-based data distribution system, choosing the right data resource for storage, as a data storage node of the system, first needs to have enough storage capacity. The system maintenance node is used to "mining," in this way to maintain the blockchain ledger of the blockchain-based data distribution system. A system maintenance node is not only be in a position of a certain amount of storage capacity and be suitable for the global ledger of storage system but also sufficient computing power is required to complete the proof of work. Ordinary nodes can also be light nodes. Such nodes have the lowest requirements on the nodes themselves. Under normal circumstances, only the account books and data related to themselves need to be stored.

4. Conclusion

In the context of big data, the inherent or potential value of data makes it an important asset. Common data in daily life generally undergoes a series of processing. Due to the lack of necessary transparency in the intermediate process, it is difficult for users to judge its source and reliability. Through the combination of blockchain technology and other scenarios and technologies, many tasks that were previously considered difficult to accomplish can be accomplished. Digital cities will inevitably require digitization of production factors and holographic economic activities to form a scalable economy. Blockchains can replace the original "face-to-face trust" relationship with "back-to-back trust," reducing the cost of transactions and exchanges. In the meantime, the "chain network" is used to unitize the blockchains of different architectures and different scenarios, realize the digitalization of the production factors, and completely record the whole process of the flow, connection, and equity distribution of social production materials. The blockchain system provides limited identity privacy and data privacy protection capabilities. This article analyzes the identity privacy and data privacy leakage problems of the blockchain system in-depth and combines privacy protection mechanisms and cryptographic algorithms to propose solutions and protections to enhance user identity privacy. The public key of data privacy can search for the blockchain data privacy protection scheme, which improves the privacy protection mechanism of the blockchain system. Based on the ecological environment of the blockchain system, using the distributed data storage function of the blockchain system can bring new application modes to a large number of field application systems. At present, various application fields have formed a preliminary accumulation in blockchain technology, gradually combining the functions of the blockchain system with the original business system, using the characteristics of the blockchain to solve the drawbacks of the business system, and at the same time, improving the blockchain system itself has shortcomings and limitations. Now, applications in various fields have presented more new challenges to the blockchain system.

This study merged the blockchain and big data together, and the big data privacy protection and scalability issues are deeply studied and analyzed based on the existing blockchain system architecture, and some research results are obtained, but there are still many works that can be further studied. According to the viewpoint of tackling the security assurance and versatility of large information sharing, this study proposes a shared data privacy protection and scalability solution. This solution solves the data storage problem to some extent, but the recorded data are still stored in the cloud. There may still be the possibility of centralization failure. The next step will be to expand the solution based on the existing research results to further solve the problem of centralization failure.

Data Availability

No data were used to support this study.

Conflicts of Interest

The author declares that there are no conflicts of interest with any financial organizations regarding the material reported in this manuscript.

Acknowledgments

This work was supported by the scientific research project of the Shaanxi Provincial Education Department in 2018 (project no. 18JK1189).

References

[1] L. Liu and B. Xu, "Research on Information Security Technology Based on Blockchain," in *Proceedings of the 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, pp. 380–384, Chengdu, China, April 2018.

[2] H.-T. Wu and C.-W. Tsai, "Toward blockchains for healthcare systems: applying the bilinear pairing technology to ensure privacy protection and accuracy in data sharing," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 65–71, 2018.

[3] H. Zhao, P. Bai, Y. Peng, and R. Xu, "Efficient key management scheme for health blockchain," *Caai Transactions on Intelligence Technology*, vol. 3, no. 2, pp. 114–118, 2018.

[4] S. Prasad, R. Shankar, R. Gupta, and S. Roy, "A TISM modeling of critical success factors of blockchain based cloud services," *Journal of Advances in Management Research*, vol. 15, no. 4, pp. 434–456, 2018.

[5] R. Qin, Y. Yuan, and F.-Y. Wang, "Research on the selection strategies of blockchain mining pools," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 3, pp. 748–757, 2018.

[6] B.-K. Zheng, L.-H. Zhu, M. Shen et al., "Scalable and privacy-preserving data sharing based on blockchain," *Journal of Computer Science and Technology*, vol. 33, no. 3, pp. 557–567, 2018.

[7] P. Mamoshina, L. Ojomoko, Y. Yanovich et al., "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *Oncotarget*, vol. 9, no. 5, pp. 5665–5690, 2018.

[8] L. Li, J. Liu, L. Cheng et al., "CreditCoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2204–2220, 2018.

[9] M. N. Kamel Boulos, J. T. Wilson, and K. A. Clauson, "Geospatial blockchain: promises, challenges, and scenarios in health and healthcare," *International Journal of Health Geographics*, vol. 17, no. 1, p. 25, 2018.

[10] 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, p. 140, 2018.

[11] M. Benchoufi and P. Ravaud, "Blockchain technology for improving clinical research quality," *Trials*, vol. 18, no. 1, p. 335, 2017.

[12] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," *IET Communications*, vol. 12, no. 5, pp. 527–532, 2018.

[13] B. D. Trump, M.-V. Florin, H. S. Matthews, D. Sicker, and I. Linkov, "Governing the use of blockchain and distributed ledger technologies: not one-size-fits-all," *IEEE Engineering Management Review*, vol. 46, no. 3, pp. 56–62, 2018.

[14] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: a data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[15] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: a systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[16] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, "IoTChain: establishing trust in the internet of things ecosystem using blockchain," *IEEE Cloud Computing*, vol. 5, no. 4, pp. 12–23, 2018.

[17] C. Kuner, F. Cate, O. Lynskey, C. Millard, N. Ni Loideain, and D. Svantesson, "Blockchain versus data protection," *International Data Privacy Law*, vol. 8, no. 2, pp. 103-104, 2018.

[18] M. Zhaofeng, H. Weihua, and G. Hongmin, "A new blockchain-based trusted DRM scheme for built-in content protection," *EURASIP Journal on Image and Video Processing*, vol. 2018, no. 1, p. 91, 2018.

[19] M. Yang, A. Margheri, R. Hu, and V. Sassone, "Differentially private data sharing in a cloud federation with blockchain," *IEEE Cloud Computing*, vol. 5, no. 6, pp. 69–79, 2018.

[20] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *Journal of Medical Systems*, vol. 43, no. 1, p. 5, 2018.

[21] R. Zinko, H. de Burgh-Woodman, Z. Z. Furner, and S. J. Kim, "Seeing is believing," *Journal of Organizational and End User Computing*, vol. 33, no. 2, pp. 85–104, 2021.

[22] M. Shemeis, T. Asad, T. Asad, and S. Attia, "The effect of big five factors of personality on compulsive buying: the mediating role of consumer negative emotions," *American Journal of Business and Operations Research*, vol. 2, no. 1, pp. 5–23, 2021.

[23] A. Sharma, Y. Sharma, R. Bansal et al., "Implementation of crowd sale using ERC-20 tokens," *Journal of Cybersecurity and Information Management*, vol. 2, no. 1, pp. 05–12, 2020.