Hindawi
Mobile Information Systems
Volume 2022, Article ID 7585288, 11 pages
https://doi.org/10.1155/2022/7585288

Research Article

Blockchain-Based Secure and Trusted Distributed International Trade Big Data Management System

Guohua Lian [1,2]

[1]*Hainan Vocational University of Science and Technology, Haikou 571126, Hainan, China*
[2]*School of Computer Sciences, Universiti Sains Malaysia, Penang 11800, Malaysia*

Correspondence should be addressed to Guohua Lian; guohua.lian@hvust.edu.cn

Received 14 July 2022; Revised 10 August 2022; Accepted 22 August 2022; Published 12 September 2022

Academic Editor: Chia-Huei Wu

As an object of rapid development of Internet technology in recent years, network security has attracted more and more attention from people from all walks of life and has gradually become a topic in international trade activities. The application of blockchain is also extremely extensive, involving many aspects, such as the development of the metaverse game engine and bank financing. With the launch of the Belt and Road strategy, trade exchanges have become more and more frequent, and at the same time, cross-border e-commerce, a new type of industry that applies Internet information technology, has emerged. The application of blockchain technology to international trade big data processing can not only improve the utilization rate of massive transaction information resources shared by enterprises, governments, financial institutions, and other institutions, but also reduce enterprise costs. The use of blockchain improves the efficiency of data storage, reduces the degree of encryption, and reduces the amount of database access and server resource occupation. This paper mainly studied the application of blockchain in international trade big data system, introduced its secure and trusted distributed network architecture, and analyzed its performance. The experimental results showed that the performance of the decentralized manager was better than that of the centralized manager when processing a large amount of data. The peak throughput of the decentralized manager was about 450 pcs/sec and the peak throughput of the centralized manager was about 150 pcs/sec. And the performance of the storage system in the local area network was better than that in the public network.

1. Introduction

Since the beginning of the twenty-first century, the Internet has entered the lives of the public at an unimaginable speed. Data has been growing rapidly, and mankind has entered the era of big data. In the context of big data, the inherent or potential value of data itself has become an important asset. Raw data is generally considered to be unprocessed or reduced data that constitutes physically present data. What people most often come into contact with in their daily life is the evolution of raw data, which has undergone a series of processing. At the same time, people are unknown to the source of this data, and they cannot judge its security and reliability. This also gives many criminals an opportunity to take advantage. If the advanced and reliable encryption algorithm (LSS) is used to realize the isolation and protection of massive data, it has become the top priority, and it also provides the digital virtual world with a feature of high security, strong reliability, and scalability. With the continuous improvement of network communication standard system requirements in the field of Internet technology and information security, a more credible blockchain alliance is proposed in this case. The purpose of the Global Blockchain Alliance is to promote the self-discipline of the global blockchain industry, promote the research and application development of global blockchain technology, build industry standards for the blockchain industry, drive the deep integration of blockchain and various economic and social fields, and jointly promote the healthy development of the blockchain industry.

International trade has various and complex characteristics. A trade integrates many roles, such as

manufacturers, customs, logistics, and end customers, and links the market demands of various countries to form an international market. Therefore, international trade is very fragmented and chaotic. The reason for the low efficiency of international trade is the lack of application of modern information technology. Blockchain is an open distributed storage system that integrates all key links that may occur or already exist, such as data sharing and access control, on a new server. A distributed system maintains a shared, public ledger of transactions. A series of transaction information data is stored in a block, each block is associated with the hash value of the previous block, and this series of blocks forms a blockchain. Due to the existence of the hash value in the transaction block, the associated transaction block cannot be manipulated without breaking the connection between the blocks. Therefore the blockchain and its distributed ledger are immutable, which makes all transactions transparent and trackable. In addition, blockchain technology can also realize direct communication between companies or individuals. This technology is decentralized and has good fault tolerance. No company or individual can unilaterally manipulate or modify the ledger, and blockchain technology is also considered safe. Therefore, the application of blockchain technology to the construction of international trade management systems can solve its security problems.

International trade is about not only whether a company is strong, but also whether a country is prosperous, so international trade has always been the focus of international scholars. Akerman [1] analyzed the leading role played by wholesalers and other intermediaries in international trade and gave corresponding management suggestions [1]. Niepmann and Schmidt-Eisenlohr [2] studied the significant risks faced by international trade exporters and importers during the financial crisis and provided their own views on how to apply letters of credit to the risks [2]. Alvarez [3] proposed to introduce the Eaton-Kortum model into international trade, aiming to use this model to evaluate the short-term and long-term benefits brought by the elimination of global trade tariffs [3]. Sopranzetti [4] analyzed the impact of free trade agreements on international trade and concluded that signing free trade agreements with each country was not the best strategy to increase trade volume [4]. McCalman [5] studied the relationship between income distribution and international integration in the trade environment and showed that when income distribution was different, it affected the gains from trade within and between countries [5]. Broll and Mukherjee [6] studied the optimal production and trade decisions of international firms facing uncertainty due to exchange rate fluctuations under mean-variance preference [6]. The above research lacks some experimental data to prove that it lacks convincing. Therefore, it is necessary to study it in combination with experimental data.

In view of the lack of experimental data in the above-mentioned research on international trade, this article adapt the in-depth topic of blockchain on international trade to build a secure and reliable distributed big data management system and proved its feasibility. International scholars have also conducted a lot of research on blockchain and distributed big data management systems. Chen [7] applied the blockchain to the personnel file information management system, which effectively solved many problems in traditional file management [7]. Chen [8] and his team pointed out the limitations of existing blockchain frameworks that hinder their widespread adoption in the business world and proposed a cryptographic sharing scheme [8]. Zhang and Zhang [9] proposed the use of blockchain to improve the utilization of agricultural big data and solve the problem of multisource data fusion [9]. Zhang [10] improved the blockchain communication technology, the main purpose of which was to optimize the efficiency of blockchain data transmission [10]. Kumar and Rahman [11] proposed a metadata blockchain distribution system, which was mainly used for distributed and massively parallel processing of big data [11]. Rassenfoss [12] explored the use of blockchain in business and proposed a system that can automatically track oil and gas costs and oilfield transportation costs [12]. Most of the above studies are the application of blockchain technology, which shows the extensive application of blockchain. This further proves the feasibility of the research proposed in this paper.

This paper mainly starts with some existing problems in international trade and proposes a method for designing and verifying a distributed management system for international trade based on blockchain technology. Due to the intricate complexity of international trade, analysis and comparison of experiments are carried out from each module of the system, and experimental conclusions are drawn.

2. Design of Secure and Trusted Distributed Management System

2.1. Overview of Blockchain and International Trade. The bottleneck in international trade is the complex and slow approval process involving multiple banks and intermediaries. For example, the normal import and export materials approval is about 30 days, and the time for preparing the approval materials in the early stage is not included. Due to the time-consuming nature of these processes, payments and shipments are regularly delayed. In addition, due to information asymmetry between trading partners from different regions and economic environments, they are vulnerable to fraud during the transaction process. International trade lacks transparency and is highly ambiguous, requiring extensive control and monitoring, while a complex environment adds to cost pressures. Logistics is an important part of international trade, and freight volume is also the biggest factor affecting international trade volume [13]. Logistics pays more attention to the physical transportation of goods, while supply chain pays more attention to the management of the overall flow of goods. The difficulty of goods flow management is that there is a large amount of data and order information to be processed.

It is the various issues involved in international trade that provide a lot of opportunities for blockchain technology. This technology has the potential to disrupt many industries. Blockchain is an open distributed ledger that

records transactions securely, permanently, and efficiently [14]. Blockchain opportunities and benefits include lower IT costs, higher data quality, greater transparency, faster business processes, lower process overhead costs, and improved collaboration. The blockchain network does not rely on the feature of central equipment, so big data can be transferred to cloud platforms or other information equipment. Even if there is a natural disaster, only the equipment will be affected. The establishment of such a system takes the government agency as the leading agency, the information is open and transparent, and the terminal is opened to the enterprise to replace the expensive data center, and the enterprise can also save a lot of budget. Each block in the blockchain is linked to the hash value of the previous block. Blockchain is the first distributed record system with its own trust mechanism and is also a decentralized data storage model [15]. The structure of each block is shown in Figure 1.

2.2. Design of Distributed International Trade Big Data Management System. The blockchain integrates asymmetric encryption technology, smart contracts, and distributed systems, which originally originated from Bitcoin [16]. Blockchain technology also has disadvantages. The waste of computing resources in the current blockchain technology is mainly caused by the repeated operations of computers to compete for new blocks. Blockchain data occupies too much storage space. Due to the distributed storage characteristics of blockchain technology, any computer node that joins the blockchain network needs to synchronize the full amount of blockchain data. The core of blockchain technology is a protocol to achieve distributed consensus [17].

To avoid the above drawbacks, an effective blockchain model needs to be designed. Distributed data and blockchain technology are built on smart contracts between responsive executors [18]. It is of great research significance to improve and overcome the abovementioned shortcomings of existing blockchain technology.

As shown in Figure 2, each database in the database layer corresponds to a blockchain network, and many blockchain networks form a blockchain system. The system is connected to the cloud data sharing module and can be independently divided into blockchain nodes. The blockchain node is connected to the node server. After the node server is encrypted, the encrypted database can be decomposed into different data and presented to the server.

2.2.1. Computing System. The computing system computes the data through task distribution and aggregation. Each computing node has two states: distribution state and computing state. The computing node actively initiates a distributed calculation and enters the distribution state, dividing the relatively large calculation into multiple computing tasks. Then other computing nodes receive instructions to perform computations, that is, computation states. Its flowchart is shown in Figure 3.

2.2.2. Storage System. The storage system is mainly responsible for the storage and output of data and establishes new blocks for the data results from the computing system. Its structure diagram is shown in Figure 4.

The blockchain storage area stores two complete blockchains, namely, the calculation result blockchain and the transaction blockchain. Calculation results of the blockchain contain all the calculation results completed by the computing network. The transaction blockchain is the user's free transaction or the corresponding transaction generated by the block in the blockchain based on the calculation result. For the calculation result block unit of each task contained in the calculation result block, there must be a corresponding block unit in the transaction block. All of these storage nodes will execute the same proof-of-work algorithm at the same time as long as there is data stored in the block-unit staging area. Only the first storage node that completes the above steps is eligible to generate new blocks, and the algorithm of proof-of-work is customized by the blockchain user.

2.2.3. Trading System. Each transaction in the transaction system structure includes a transaction head and has multiple inputs and multiple outputs at the same time, as shown in Figure 5.

Every input in a transaction is an output of another transaction, and these outputs contain all the available outputs of the originator. Each output contains the output's transaction status, transaction amount, lock script, and recipient. The transaction status indicates whether the transaction is available or not. The transaction status has two values, 0 and 1. 1 means available and 0 means unavailable. Recipient is the address of the recipient of this output. A lock script is the "lock" for the transaction: if the lock script exists, the transaction is available; otherwise it is unavailable. The lock script is the transaction amount encrypted with the receiver's public key, and only the receiver's private key can unlock the script.

Assuming that the transaction amount is B, the receiver's public key is KQ, the receiver's key is KT, the lock script is lock, and the transaction status is V, the locked script can be expressed as formula (1):

$$\text{lock} = \begin{cases} RSA\text{Encrypt}(B, KQ), & V = 1, \\ \text{NULL}, & V = 0. \end{cases} \tag{1}$$

If the locked script is NULL, the script for locking the door has been unlocked, and the corresponding output is not available. The transaction status can be expressed as formula (2):

$$V = \begin{cases} 1, & RSA\text{Decrypt}(\text{lock}, KT) = B, \\ 0, & RSA\text{Decrypt}(\text{lock}, KT) \neq B. \end{cases} \tag{2}$$

Among them, RSADecrypt stands for RSA decryption. Each input in a transaction contains the block depth and transaction number of its corresponding output. The block depth and transaction number can identify unique outputs.

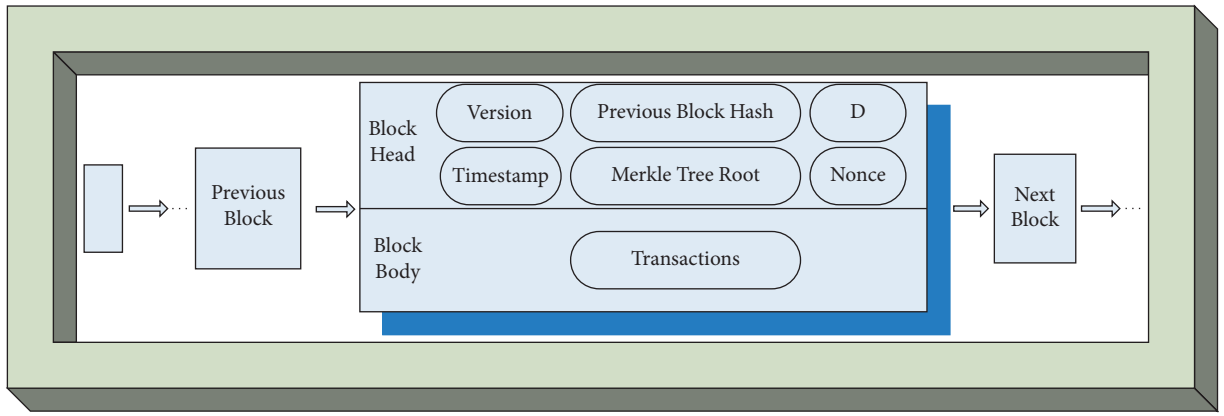

Figure 1: Schematic diagram of blockchain structure.

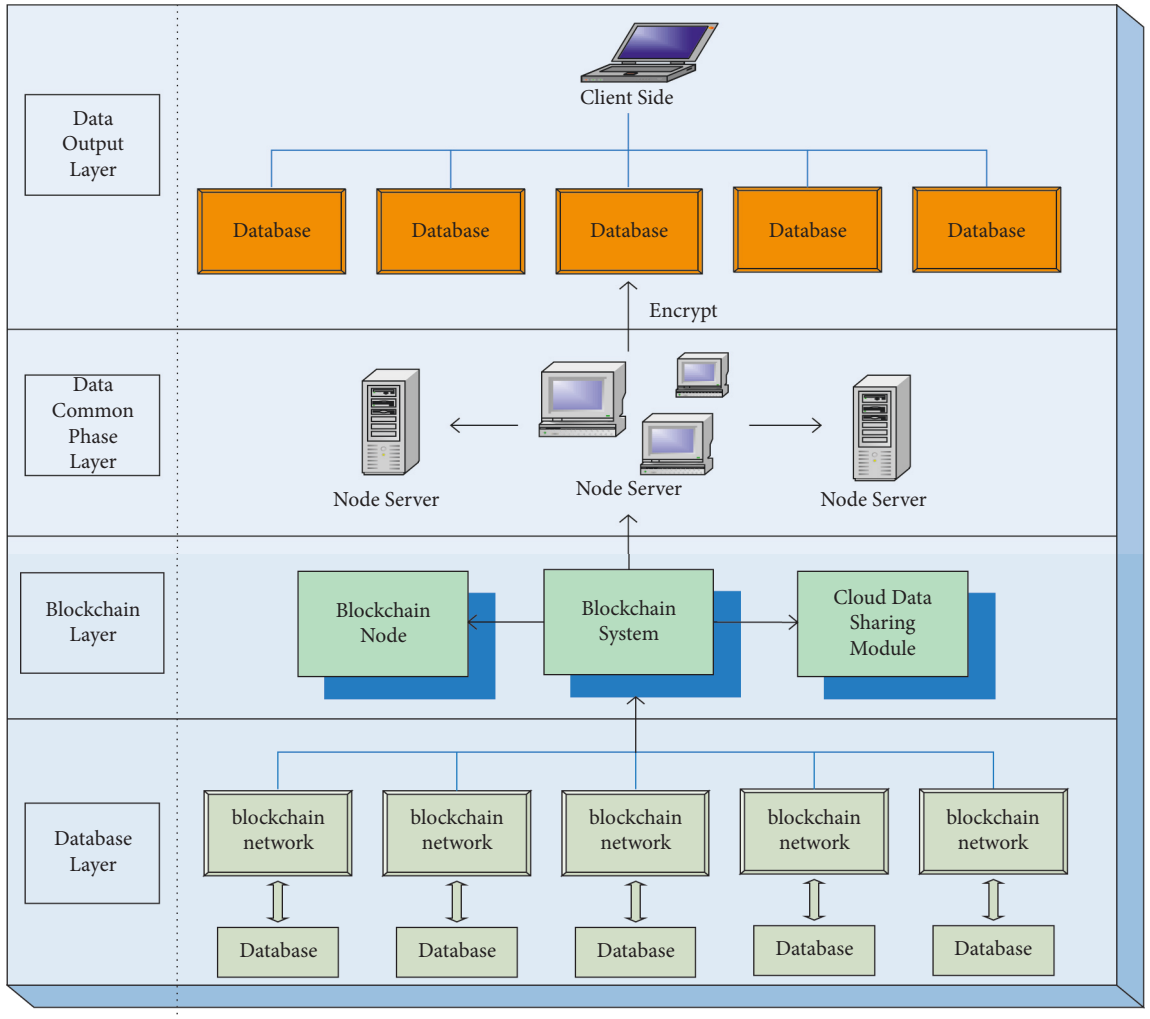

Figure 2: Schematic diagram of blockchain distributed data management system.

The transaction header contains the transaction number, originator, and hash value. The transaction number identifies the position of the transaction in the block, and the transaction number in each block increases sequentially from 1. The initiator is the public key of the transaction initiator, which is the unique identifier of the transaction initiator's identity. The transaction is divided into different data blocks according to size and stored in different nodes. When retrieving files, Merkle trees are used to retrieve data blocks on different nodes [19]. Suppose there are m inputs

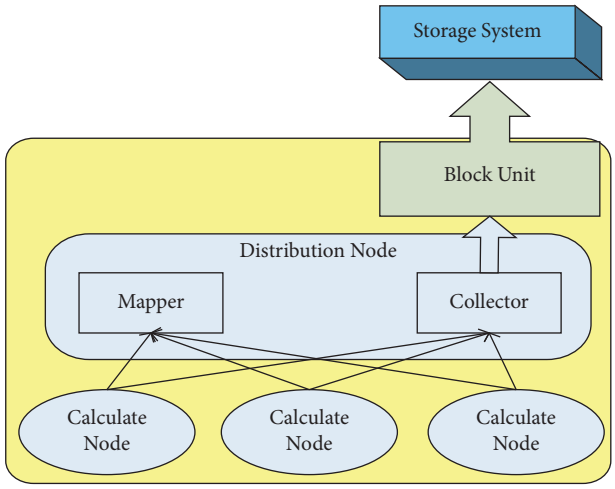

Figure 3: Schematic diagram of the computing system structure.

and n outputs in a transaction, denoted as $A_1, A_2, \ldots, A_m$ and $C_1, C_2, \ldots, C_n$, respectively. The depth of the block where the output corresponding to the input is located is D, the corresponding transaction number is M, and the hash value is H; then the hash value can be expressed as formula (3):

$$H = SHA256\left(SHA256\sum_{i=1}^{n}\left(B_{C_i} + KQ_{C_i}\right) + \sum_{i=1}^{n}\left(D_{A_i} + M_{A_i}\right)\right). \quad (3)$$

The lock script becomes NULL after unlocking and does not participate in the calculation of the hash value. The transaction status, as an identifier that may change, is only used to increase the efficiency of the transaction status query and does not participate in the calculation of the hash value.

The block header of each transaction block contains the block depth, block hash, parent block hash, timestamp, Merkle root, and transaction count. The Merkle tree operation process generally hashes the data of the block body in groups and inserts the generated new hash value into the Merkle tree, recursively until only the last root hash value is left, which is recorded as the Merkle root of the block header. The block depth represents the number of the block in the transaction blockchain. Block hash is a mathematical summary of the information present in the block. Assuming that the hash value of the block is H_x, the block contains m transactions, and the hash values are $H_1, H_2, \ldots, H_n$, respectively, the hash value of the block can be expressed as formula (4):

$$H_x = SHA256\left(\sum_{i=1}^{m}\left(H_i\right)\right). \quad (4)$$

The block hash is the key to making the blockchain immutable. The calculation of the block hash is encrypted using SHA256, a one-way irreversible encryption. And any slight change in the data in the block will cause a dramatic change in the result of SHA256 encryption. Assuming that the result type in the calculation result is F_t, the result number is F_l, the algorithm number is F_c, the initiator is F_s, there are n subtasks in the calculation result, the number of each subtask is L, the executor's public key is K, and the timestamp is T and the calculation result is F, then the hash value H of the calculation result can be expressed as formula (5):

$$H = SHA256\left(F_t + F_l + F_c + F_s + \sum_{i=1}^{n}\left(L_i + K_i + T_i + F_i\right)\right). \quad (5)$$

The IP address of the executor in the subtask is only used as a reference for the node to turn around when the character is calculated and does not participate in the calculation of the hash value.

2.2.4. Blockchain Distributed Data Access. Data access includes the transaction ledger of the blockchain, public and private key encryption, and encrypted hash function [20]. Secure storage of data requires the use of blockchain to store the IPFS hash address of the provenance data [21]. In the data upload stage, the data owner first selects the data to be shared, generates the receiver key KQ to encrypt the data, and then obtains the encrypted information JM. Policy tree is a way to store all elements in a hash table [22]. Attribute permission public key, system parameters, and policy trees are encrypted with keys, as shown in formulas (6) and (7):

$$\text{EncryptData}\left(D, KT\right) \longrightarrow JM, \quad (6)$$

$$\text{AuthEncrypt}\left(PK, T, KT, GP\right) \longrightarrow CI. \quad (7)$$

The data owner obtains the metadata data name MData, the data keyword DKData, the ciphertext request access policy req_policy according to the data, and the encrypted information EI, which constitutes the metadata set NIData and is registered in the data management contract, as shown in formula (8):

$$NI_{\text{Data}} = \{M_{\text{Data}}, DK_{\text{Data}}, EI, \text{reqpolicy}\}. \quad (8)$$

The data requester determines the target data acquisition JM. The data requester calls the data request contract to obtain the encrypted data information EI and requests the user public key KQ from the attribute agency A and decrypts to obtain the data key KT, as shown in formula (9):

$$\begin{cases} \text{Decrypt}\left(KQ, EI, GP\right) \longrightarrow KT \\ \text{DecryptData}\left(JM, KT\right) \longrightarrow D \end{cases}. \quad (9)$$

The access control mechanism algorithm flow mainly includes four stages, initialization stage, ciphertext publishing stage, data request stage, and data decryption stage. In the early stage of system establishment, it is necessary to construct an N-stage bilinear group F, where $N = q_1q_2q_3$, q_i is a prime number, and k represents a bilinear map. From F, the generator f of its subgroup Fq_1 is obtained. In addition, a random digest function H is constructed as a user identity map. The initial algorithm of system establishment is shown in formula (10):

$$FQ\left(N, f\right) \longrightarrow \text{Setup}\left(\lambda\right). \quad (10)$$

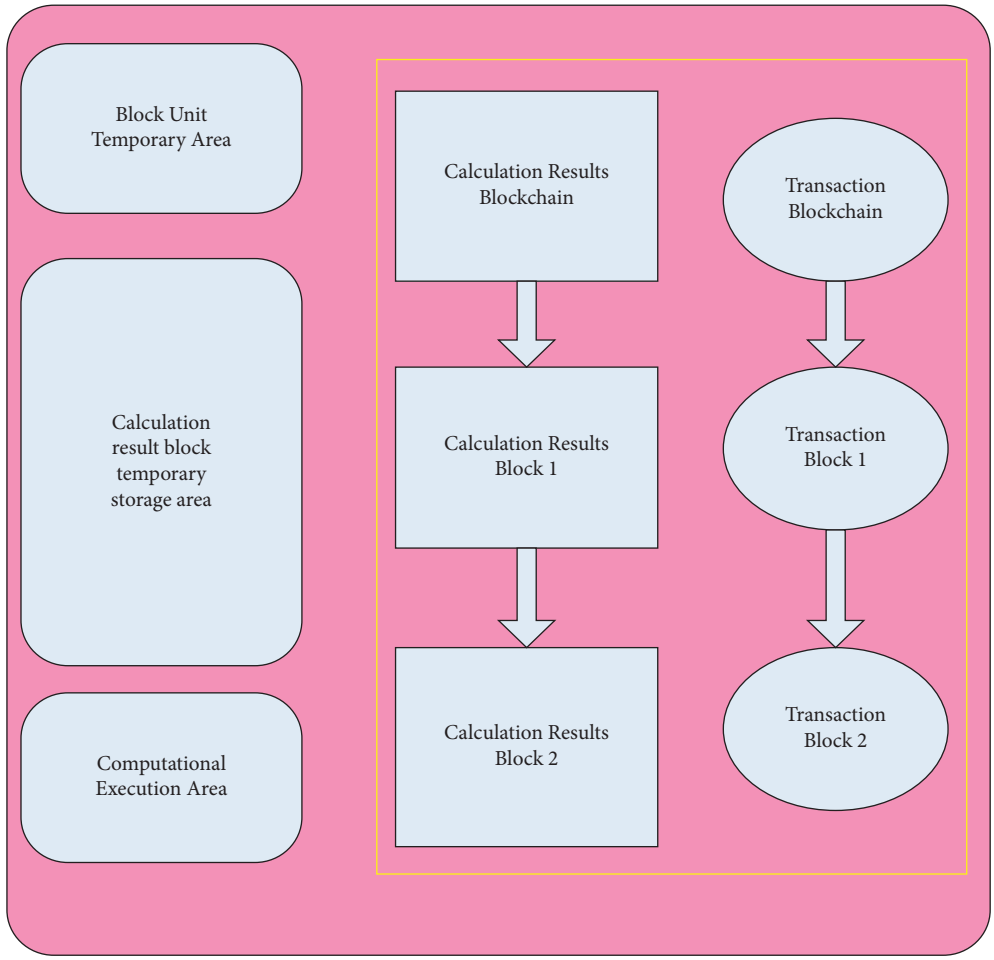

Figure 4: Schematic diagram of storage structure.

In the initialization phase, the attribute authority A calls the authorization initialization phase method and selects two random indices $\alpha_i, \gamma_i \in Z_q$ for each attribute i in the attribute set U. Taking the public system parameter GP and the attribute space U as input, the authority key KT and the authority public key KQ_j are obtained, and the attribute authority issues the authority public key through the attribute management contract and registers the attribute set U, as shown in formula (11):

$$\begin{cases} (NK, KQ) = \mathrm{AuthKeyGen}(\lambda, U) \\ KQ = \left(e(f,f)^{\alpha_i}, f^{\gamma_i} \forall i\right) \\ KT = \left(\alpha_i, \gamma_i \forall i\right) \end{cases}. \tag{11}$$

In the ciphertext publishing phase, the policy maker needs to encrypt the information N. The preorder expression T of the input policy tree is transformed into the LSSS permission matrix $(C_{m\ell}, \rho)$. The global parameter GP and the authority public key KQ are used to obtain the information ciphertext JM. After the policy maker obtains the ciphertext of M, it calls the data management contract and uploads CT to the chain state database. Its expression is as in formula (12):

$$JM = \mathrm{Encrypt}\left(M, \left(C_{m\ell}, \rho\right), GP, KQ\right). \tag{12}$$

First, the strategy makers select a random number $s \in Y_q$ and a random vector $\overrightarrow{v} \in Z_M^{\ell}$ whose first element is s and select a random vector $\overrightarrow{\omega} \in Z_M^{\ell}$ whose first element is 0. The expressions of the two vectors are as shown in formula (13):

$$\left.\begin{aligned} \overrightarrow{v} &= \left(s, a_2, a_2, \cdots a_i\right)^T \\ \overrightarrow{\omega} &= \left(0, b_2, b_2, \cdots b_i\right)^T \end{aligned}\right\} \in Z_M^{\ell}. \tag{13}$$

EO picks a random number of $r_x \in Z_q$ for each row. The expression that can calculate the ciphertext JM is as shown in formula (14):

$$\begin{cases} J_0 = M \cdot e(f,f)^s \\ J_{1,y} = e(f,f)^{\lambda_x} e(f,f)^{\alpha_{\rho(x)}\gamma_x} \\ J_{2,y} = f^{\gamma_x} \\ J_{3,y} = f^{\alpha_{\rho(x)}\gamma_x} \cdot f^{\omega_x} \\ JM = \left\{J_0, \left(J_{1,y}, J_{2,y}, J_{3,y}\right), (A, \rho)\right\} \end{cases}. \tag{14}$$

The controlled requester locates the specific data and requests the encrypted information JM from the data

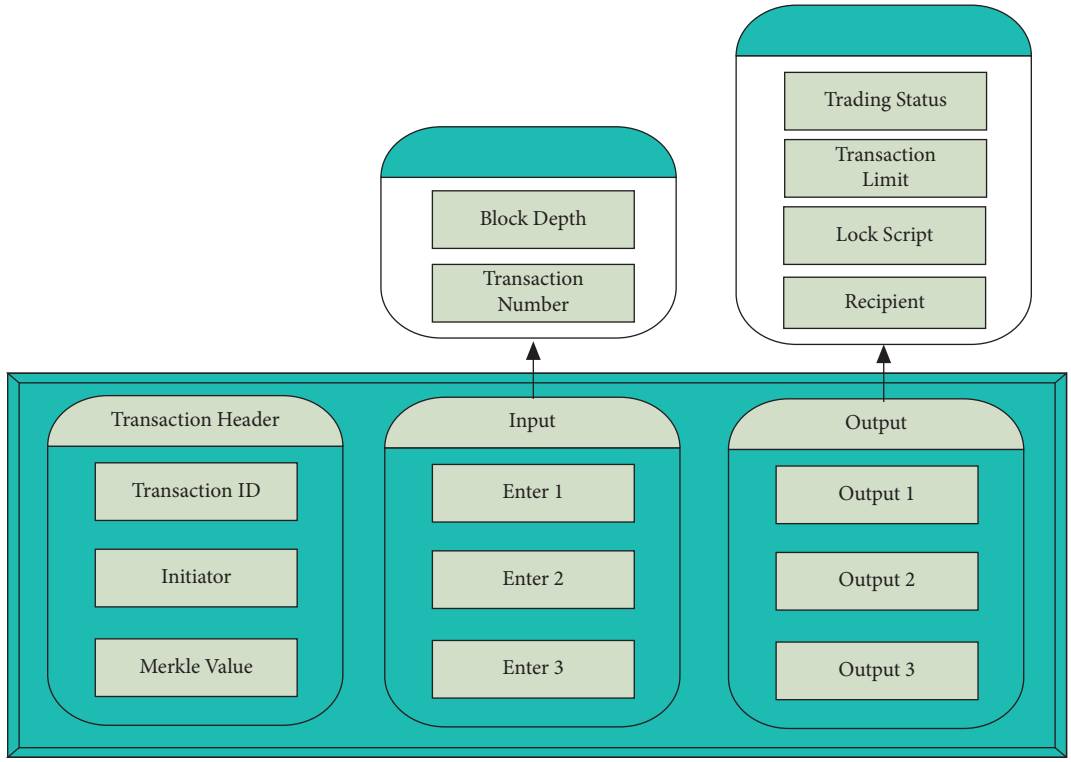

Figure 5: Schematic diagram of the trading system structure.

management contract. The data requester calls the data request contract to apply to A for JM. First, the data request contract calls the data management contract to obtain the dynamic access policy DPData and determines the user's authority according to the user's current dynamic attributes. ATTR is a user ciphertext request attribute set, which is a dynamic attribute set. The dynamic attribute ATTR refers to information that changes with time or the location of the data requester, such as the current access timestamp, the Internet Protocol address of the current controlled requester, and other dynamic information. The expression of ATTR is as formula (15):

$$\text{ATTR} = (attr_1, attr_2, \ldots \text{attr}_k). \tag{15}$$

For the control requester's dynamic information chain judgment as the user ciphertext request permission verification, the data request contract decides whether to apply for the user system ciphertext JM to the data requester according to the access attribute judgment result can_access. If it is can_access, the value is 1, and the JM can be returned to the user; otherwise the user request is denied. The access request contract decidePolicy is decided as in formula (16):

$$\begin{cases} \text{canaccess} = \text{decicidePolicy}(\text{ATTR}) \\ \text{canaccess} = \begin{cases} 1, \text{ok} \\ 0, \text{deny} \end{cases} \end{cases}. \tag{16}$$

The controlled requester requests the user key Ki, GID and related information Ti, GID from the attribute authority. The property authority party encrypts the key-related information using the KQ public key pubkey and sends it to KQ. The generation of Ki, GID and Ti, GID is shown in formula (17):

$$\begin{cases} \left(K_{i,\text{GID}}, T_{i,\text{GID}}\right) = \text{UkeyGen}(GID, KQ, KT, i) \\ K_{i,\text{GID}} = f^{\alpha_i} H(GID)^{\gamma_i} \\ T_{i,\text{GID}} = H(i)^{\ell} \end{cases}. \tag{17}$$

If the controlled requester passes the data request permission determination, it will obtain the JM and the key and related information. First, the decryption algorithm is executed locally to obtain the user system key Ki, GID. The controlled requester executes the decryption algorithm and decrypts the encrypted information JM through the user key Ki and GID. The decryption algorithm is shown in formula (18):

$$\begin{aligned} M &= \text{Decrypt}\left(JM, K_{i,\text{GID}}\right), \\ d_x &= \frac{J_{1,y} \cdot e\left(H(GID), J_{3,y}\right)}{e\left(K_{\rho(y)}, J_{2,y}\right)}, \\ M &= \frac{J_0}{\prod_x d_x^{j_y}} = \frac{J_0}{e(f,f)^s}. \end{aligned} \tag{18}$$

3. International Trade System Evaluation Experiment

3.1. System Function Test Experiment. In this paper, the system function test is carried out on the system model, and

Table 1: Server and client device configuration table.

Name		Server configuration	Software
Blockchain server side	Server 1 ~ 5	CPU core: 4 RAM: 8G CPU frequency: 2.50 GHz Centos 7.5	Golang 1.11
Client side	Laptop 1	CPU core: 4 RAM: 8G CPU frequency: 2.50 GHz Centos 7.5	Java 1.8
	Laptop 2	CPU core: 4 RAM: 8G CPU frequency: 2.50 GHz Centos 7.5	Java 1.8

Table 2: Test data information table.

Type	Name	Data
Identity information	Lucy	User Id: User 1 Username: Lucy User corner: Normaluser organization information: Org 1
	Jessica	User Id: User 2 Username: Jessica User corner: Normaluser organization information: Org 2
	Monica	User Id: User 3 Username: Monica User corner: Normaluser organization information: Org 1
Property agency	No.1	Property Agency Id: A1; Attribute Information:{a : 111222; b : 466313} User attribute Information:{Lucy : a; Monica : b}
	No.2	Property Agency Id: A2; Attribute Information:{c : 15646; d : 97344} User attribute Information:{Jessica : c, d}

the required test data is given first in the test. The test data has the function of managing the data and the function of the test data requester requesting the data to see if it meets the expectations. Three different servers are configured and selected, and the selected configuration must be representative. The configuration selected this time is the computer configuration used in normal office work. The advantage of this is that there is no need to worry about the configuration problem affecting the functionality of the system. The specific device configurations of the server and client are shown in Table 1.

In the functional test, three users need to be registered for login, and then two attribute organizations are created and responsible for the corresponding attribute information. The specific test data is shown in Table 2.

This paper uses the identity of one of the ordinary users to test the data owner management data, and the obtained test results are shown in Table 3.

From the experimental results, it can be known that the expected functional effects can be achieved by performing different operations on the three different management rights of the data owner. The purpose of this experiment is to test whether the management authority of the data owner can be used normally when the system is running normally, which also proves the security and indirectness of the system data mentioned above.

3.2. System Performance Test. Through the functional test of the system, it can be found that the designed system model can achieve the expected functional effect. Management systems involve access and user privacy issues between digital authentication and authorization [23]. Therefore, in order to further improve the feasibility of the theory, the performance test of the system is mainly aimed at the test of the manager terminal. The experiment uses java language to simulate the client. The throughput of the decentralized authorization manager and the central authorization manager under the data transaction request volume is compared. The comparison of the experimental results is shown in Figure 6.

It can be seen from Figure 6 that, with the continuous increase in the amount of data transaction requests, the throughput of the decentralized authorization manager processing data transactions was generally linearly increasing and finally reached a peak value around 450 pcs/sec. The overall linearity of the throughput of the central authorization manager processing data transactions was slow and finally peaked at about 150 pcs/sec. Central authorization manager processing has certain advantages over decentralized authorization managers. The throughput of the two points is similar when the transaction volume is small. This is because when dealing with a small transaction volume, the blockchain does not need to perform repeated calculations to generate new blocks, so the throughput of the two is similar.

Then the performance of encryption and decryption of the system was tested. The length of the encrypted information was fixed, and three attribute mechanisms were

Table 3: Data owner managed data test results table.

Test	Operate	Expected	Result
Test whether users can encrypt data content	Monica uploads the data file test data and symmetric key and clicks the data encryption button	The data content is encrypted and can be decrypted using the symmetric key to obtain the original data file	Accord
Test whether users can modify data information	Lucy modifies data information	The data information in the blockchain state database is modified	Accord
Test whether nondata owner users can modify data information	Jessica modifies data information	Nondata owners cannot modify data information	Accord

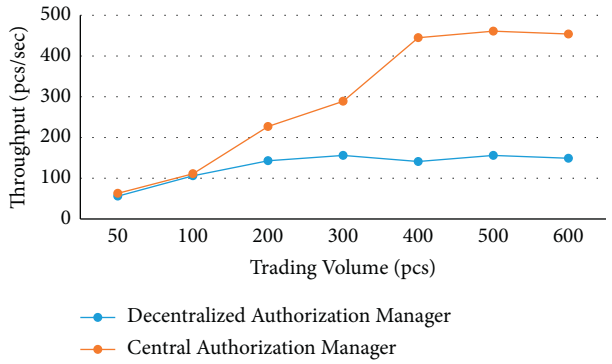

Figure 6: Comparison of processing data transaction throughput in two modes.

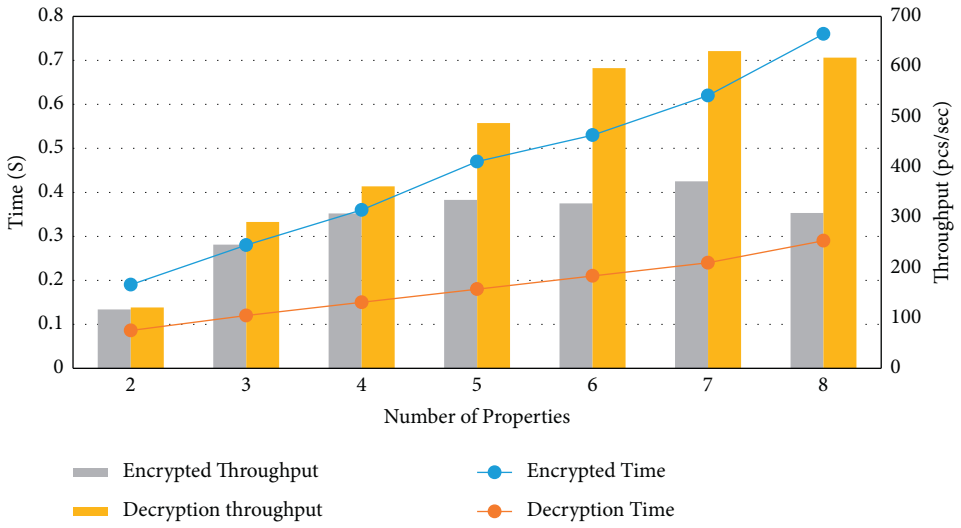

Figure 7: Encryption and decryption performance test chart.

selected in each database. To test the performance of the encryption/decryption module under different attribute amounts, five tests were carried out for each attribute organization and the average value was obtained. The test results are shown in Figure 7.

It can be seen from Figure 7 that the encryption and decryption time increased with the increase of the number of attributes. In addition, the attribute amount had a great influence on the encryption function, and the processing efficiency of the encryption time was greatly reduced with the increase of the attribute amount. From the histogram comparison, it can be seen that the throughput of the encryption function is not very obvious with the increase of the number of attributes. However, the throughput of the decryption function has increased significantly. This is because when the data is stored in the cloud database, the total number of terminal servers is less than the total number of clients, and the encryption process is more complicated and

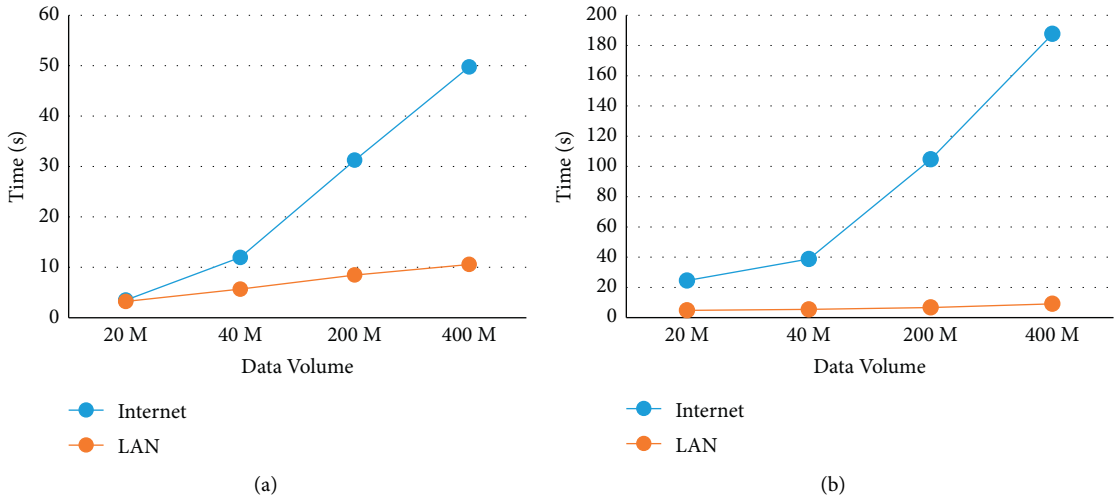

Figure 8: Storage module performance test. (a) Data upload performance test. (b) Data download performance test.

involves digital identity authentication. And the peak throughput of the encryption function was about 370 pcs/sec, and the peak throughput of the decryption function was about 600 pcs/sec.

Storage modules are at the heart of determining a system model. Therefore, the performance test of the storage module was carried out on the system model to test the upload and download of data, and the data with the data volume of 20 M, 40 M, 200 M, and 400 M were tested on the Internet and LAN, respectively. The comparison chart of the experimental results is shown in Figure 8.

From the performance comparison chart of experimental data upload and download, it can be seen that the data write rate and read rate were basically stable with the increase of the data volume under the LAN. However, the efficiency of reading memory in the public network environment was gradually declining, and the user's performance bottleneck for data sharing still existed in the data upload and download parts of the public network environment. There was little difference between data writing and chain code invocation and query time through the blockchain engine. As the amount of data increased, the time for data owners to share data and data requesters to request data increased. If a user downloaded data on the public network under the same local area network, the rate at which other users in the local area network download data was greatly increased. Therefore, this paper can verify that the overall performance of the system meets the requirements for data security sharing of daily life and work data.

4. Conclusions

Blockchain is a disruptive technology whose impact is comparable to the introduction of the World Wide Web. The technology focuses on the interaction of enterprises and people, breaking down organizational silos, reducing management costs, improving communication within companies, and improving communication among various participants in international trade. Blockchain technology also establishes a trustless way of doing business. It improves the overall efficiency of international trade and can completely replace middlemen and entire supply chains based on inefficiencies. Through experimental verification, it can be found that blockchain technology can improve data quality, improve transparency, speed up business processes, and improve collaboration, with better risk management and better data security. At the same time, the system model is compared in different modes and in different network environments. It can be seen that the system performs well in data processing. The decentralized data manager has better processing performance, which is several times more efficient than the centralized manager. The decentralized data manager peaks at about 450 pcs/sec, and the centralized data manager peaks at about 150 pcs/sec. The peak throughput of the encryption function is about 370 pcs/sec, and the peak throughput of the decryption function is about 600 pcs/sec. Moreover, the blockchain itself is a decentralized storage model, which further proves the research direction of this paper.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

Acknowledgments

The author received no financial support for the research, authorship, and/or publication of this article.

References

[1] A. Akerman, "A theory on the role of wholesalers in international trade based on economies of scope," *Canadian Journal of Economics/revue Canadienne Déconomique*, vol. 51, no. 1, pp. 156–185, 2018.

[2] F. Niepmann and T. Schmidt-Eisenlohr, "International trade, risk and the role of banks," *Journal of International Economics*, vol. 107, pp. 111–126, 2017.
[3] F. Alvarez, "Capital accumulation and international trade," *Journal of Monetary Economics*, vol. 91, pp. 1–18, 2017.
[4] S. Sopranzetti, "Overlapping free trade agreements and international trade: a network approach," *The World Economy*, vol. 41, no. 6, pp. 1549–1566, 2017.
[5] P. McCalman, "International trade, income distribution and welfare," *Journal of International Economics*, vol. 110, pp. 1–15, 2018.
[6] U. Broll and S. Mukherjee, "International trade and firms' attitude towards risk," *Economic Modelling*, vol. 64, pp. 69–73, 2017.
[7] J. Chen, Z. Lv, and H. Song, "Design of personnel big data management system based on blockchain," *Future Generation Computer Systems*, vol. 101, pp. 1122–1129, 2019.
[8] H. Chen, H. L. Wu, C. C. Chang, and L. S. Chen, "Light repository blockchain system with multisecret sharing for industrial big data," *Security and Communication Networks*, vol. 2019, no. 12, pp. 1–7, Article ID 9060756, 2019.
[9] F. Zhang and Y. Zhang, "A big data mining and blockchain-enabled security approach for agricultural based on Internet of things," *Wireless Communications and Mobile Computing*, vol. 2020, no. 1, pp. 1–8, 2020.
[10] J. Zhang, "Interaction design research based on large data rule mining and blockchain communication technology," *Soft Computing*, vol. 24, no. 21, pp. 16593–16604, 2020.
[11] D. S. Kumar and M. A. Rahman, "Simplified HDFS architecture with blockchain distribution of metadata," *International Journal of Applied Engineering Research*, vol. 12, no. 21, pp. 11374–11382, 2017.
[12] S. Rassenfoss, "Testing a system where machines decide how much to pay a trucker, and send a check," *Journal of Petroleum Technology*, vol. 71, no. 11, pp. 36-37, 2019.
[13] R. V. Fedorenko, "Problems of developing the customs and logistics infrastructure of the east-west international transport corridor," *RUDN Journal of Economics*, vol. 28, no. 3, pp. 491–504, 2020.
[14] M. Iansiti and K. R. Lakhani, "The truth about blockchain," *Harvard Business Review*, vol. 95, no. 1, pp. 118–127, 2017.
[15] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "IoT information sharing security mechanism based on blockchain technology," *Future Generation Computer Systems*, vol. 101, pp. 1028–1040, 2019.
[16] S. Maiyya, V. Zakhary, D. Agrawal, and A. E. Abbadi, "Database and distributed computing fundamentals for scalable, fault-tolerant, and consistent maintenance of blockchains," *Proceedings of the VLDB Endowment*, vol. 11, no. 12, pp. 2098–2101, 2018.
[17] D. Katsaros, "Distributed ledger technology: the science of the blockchain," *Computing Reviews*, vol. 59, no. 11, pp. 596-597, 2018.
[18] X. Yang, Y. Zhang, J. Lu, B. Zhao, and H. Pan, "Blockchain-based automated demand response method for energy storage system in an energy local network," *Proceedings of the CSEE*, vol. 37, no. 13, pp. 3703–3716, 2017.
[19] S. P. Yazhini and S. Santhiya, "Reliability and confidentiality based data storage in cloud using merkle hash tree technique," *International Journal of Pure and Applied Mathematics*, vol. 118, no. 9, pp. 793–799, 2018.
[20] X. Zhang, J. Grannis, I. Baggili, and N. L. Beebe, "Frameup: an incriminatory attack on Storj: a peer to peer blockchain enabled distributed storage system," *Digital Investigation*, vol. 29, pp. 28–42, 2019.
[21] J. T. Hao, Y. Sun, and H. Luo, "A safe and efficient storage scheme based on blockchain and IPFs for agricultural products tracking," *Journal of Computers*, vol. 29, no. 6, pp. 158–167, 2018.
[22] Z. Wu and K. Li, "VBTree: forward secure conjunctive queries over encrypted data for cloud computing," *The VLDB journal*, vol. 28, no. 1, pp. 25–46, 2019.
[23] T. Hardjono, "Federated authorization over access to personal data for decentralized identity management," *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 32–38, 2019.