Hindawi
Mobile Information Systems
Volume 2021, Article ID 5250512, 11 pages
https://doi.org/10.1155/2021/5250512

Research Article

Big Data Security and International Settlement System of Electronic Economy Based on Blockchain

Ying Liu, Yan Jin, and Qi Liu

College of Economic and Management, The College of Post and Telecommunication of WIT, Wuhan 430000, Hubei, China

Correspondence should be addressed to Qi Liu; 92000243@wit.edu.cn

Received 27 August 2021; Revised 25 October 2021; Accepted 30 October 2021; Published 22 November 2021

Academic Editor: Sang-Bing Tsai

In recent years, the rapid development of e-commerce and mobile communications has ushered in a new era in the era of big data and has also given birth to emerging industries such as big data. People are paying more and more attention to data, and all walks of life are trying to analyze data and make use of the potential value of data. Business organizations use big data analysis to reduce business costs, plan real-time traffic routes for thousands of express vehicles to avoid congestion, and use click stream analysis and data mining to avoid fraud. This article combines big data with e-commerce security, deeply studies the composition of e-commerce security system and key security strategies and technologies, and discusses some problems in the combined application of blockchain and electronic settlement. The birth of big data technology can solve the contradictions in today's e-commerce security, introduce the popular and widely distributed Apache Hadoop platform, deeply study the structure of Hadoop, and focus on the data analysis and processing method products of the second generation of Hadoop YARN. It is recommended to start with data, manage, and monitor e-commerce behaviors and improve the e-commerce security system. Finally, many important aspects that need to be considered in the big data e-commerce security system will be discussed. The analysis results show that the credential management and control system based on blockchain technology proposed in this paper can resist most frauds and realize the safe storage of transaction data and cannot be tampered with. Experiments have proved that the types of vulnerabilities and defects show that improper input is the main reason; the system error rate is mainly concentrated at 0.50%, and all the data indicate that the application of big data blockchain in electronic settlement provides great value, and the security of the electronic economy has increased by at least 60%.

1. Introduction

The rapid development of electronic network technology has enabled international trade to move towards efficient, safe, and low-cost online operations in the past two years. After more than 5 years of preparations, a BOLERO network that is based on the Internet and supports all parties involved in the international trade process to transmit and exchange electronic documents and data has been established and started to operate. It not only solves the problem of inconvenience for the consignee to pick up the goods because the traditional bill of lading arrives at the port of destination later than the ship but also has certain transaction security, so it has broad application prospects [1, 2]. The development of society, the progress of the times, and the innovation of Internet technology have completely changed the traditional forms of trade and promoted the rapid development of most industries including e-commerce, modern logistics, and electronic payment. Today, when cross-border e-commerce is gaining momentum, e-payment not only constitutes the core link of e-commerce but also attracts important industries at all levels of transactions and trade with its convenience and security. In recent years, the development of electronic payment models has entered a bottleneck state, which includes multiple issues such as payment methods, information transmission, and information credibility. In the current Internet and information technology era, if there is no electronic payment, e-commerce will not achieve further rapid development, and the development of modern cross-border e-commerce has put forward higher demands for the development of electronic payment. It can not only save space and time cost but also ensure the authenticity of payment information, strengthen the security of payment information, and increase the means of transmission of trade information, which will all become problems that need to be solved urgently in the development of electronic payment models [3].

From the perspective of historical development, it is critical to first explain the development model of the electronic economy. The electronic application of business documents began in the 1960s, but people used telegrams to send business documents for business activities. Later, as technology progressed, the invention of the facsimile machine replaced the telegraph. With the maturity of computer technology, in the 1980s and 1990s, the development and application of information systems can already be processed electronically. This is the early EDI (Electronic Data Interchange) and the early interenterprise e-commerce. The real application of modern electronic payment is based on the emergence and development of Internet technology after the 1990s. In the beginning, the role of the Internet was limited to browsing goods, and it did not constitute a real electronic payment method. With the further development of financial enterprises and Internet information networks, electronic checks, electronic money, and electronic banks have gradually formed application technology models. This laid the technical foundation for the modern electronic payment model and truly realized the integration and practical application of online transactions and offline delivery. This has led to the gradual development of e-finance and corporate payment models such as online banking, gateway payment, and third-party payment. As a result, the blockchain electronic economy has also obtained a huge development, and the security liquidation and other issues derived from it have been solved with the abovementioned tracing back to the source [4, 5].

Jin Yong believed that in the era of big data, the exchange of big data can effectively solve the phenomenon of "data island," data resources can also be effectively integrated, and decentralization, transparency, autonomy, anonymity, and information cannot be changed. The other natural characteristics of the company can promote the secure exchange of big data. In addition, a large amount of government data has huge economic and social value, and the safe disclosure of large government data is essential for transforming the government and changing social demand patterns. However, big data algorithms need continuous improvement to keep up with the society [6]. In the era of big data, data exchange has become more and more convenient, but there are more and more security problems caused by unnecessary data mining. Especially large-scale medical data usually involve privacy, and the leakage of these data can cause great harm to individuals and countries. Therefore, improving the security of medical data storage and communication has become a very important issue. Based on blockchain technology, the author analyzed the three levels of technology, system, and law, discussed the application of blockchain technology in medical data management, and proposed his own solutions. However, this solution has no actual experimental support, and a large number of experiments should be carried out to prove the feasibility of the solution [7]. Wang Jingwei believed that in the Internet era, large amounts of data are created every day, and complex issues such as privacy and ownership will arise during data exchange. Blockchain is a decentralized distributed data storage technology introduced in the blockchain field. The data market can eliminate these drawbacks, but at the same time, the distributed data market also brings security and privacy issues. The industry status and market research progress of mass data exchange at home and abroad have been investigated. It is necessary to meet the type of transportation platform and conduct mass data exchange based on blockchain. However, there are problems with the algorithm, errors will occur, and continuous improvement is needed [8]. Blockchain is a new application mode of computer technology such as distributed data storage, point-to-point transmission, consensus mechanism, and encryption algorithm. If the blockchain is used as a state machine, each transaction is an attempt to change the state, and the block generated by each consensus is the participant's confirmation of the result of the state change caused by all transactions in the block.

By building an electronic invoice cloud platform based on blockchain technology, it can make full use of blockchain decentralization, consent algorithms, and distributed emission functions. This will help alleviate the pain of the electronic invoice ecology. First, the decentralized function of blockchain technology is used to perform distributed blockchain-based storage, and it is ensured that all nodes become reliable data streams after being calculated by the encryption algorithm. The public ledger jointly solves the problems of duplicate rewards, duplicate electronic invoices, and data inconsistencies. Third, electronic invoices include issuers, recipients, and consumers. The proliferation of distributed blockchain networks is used to avoid inconsistencies in electronic invoice data, avoid data leakage, and improve data accuracy and efficiency. Based on the research of electronic invoices, cloud computing, and blockchain, this article proposes a feasible plan for constructing a blockchain-based electronic invoice cloud platform, describes the application process of the platform in detail, and then discusses the possible occurrences. The main issues have been explained systematically, hoping to provide new ideas for the comprehensive promotion of electronic invoices in our country.

2. Development Method of Big Data Security Sharing System

2.1. Blockchain Cloud Platform Construction. Strictly speaking, big data is not a new technology. However, there are endless methods to study big data, and it is not a new product because big data has always existed, but today it has a larger volume and is more likely to attract our attention. In fact, big data is a new kind of thinking and new understanding, and it is a stage that must go through between quantitative changes and qualitative changes. This subject aims to study the composition strategy of the current e-commerce security system, including the security technologies used in the four-layer structure: firewall technology, antivirus technology, VPN technology, NIDS system, encryption technology, encryption algorithm, security authentication, and data security protocol. Check the security threats faced by e-commerce, understand the widely used security measures, and look for the existing problems [9, 10]. The blockchain asymmetric encryption mechanism is shown in Figure 1.

As more and more applications become service-oriented, the functions provided by these applications can be used by new applications. Although these applications mainly provide services for end users, it also makes them part of the application platform. The cloud platform is composed of cloud servers equipped with cloud platform server-side software, cloud computers equipped with cloud platform client software, and network components. It is used to improve the overall performance of low-configuration or old computers to achieve current popularity speed. Taking the characteristics of data in the era of big data as the starting point and according to the core value of data in the era of big data, a hierarchical analysis of the e-commerce security system is carried out in a big data way of thinking. At the same time, it will focus on big data analysis and distributed frameworks such as HADOOP and understand its workflow and parallel processing principles and operating principles of MapReduce, HDFS, HBASE, and other subprojects. The algorithms and application practices of big data processing are researched, the unstructured data processing flow is mastered, the application of typical natural language processing methods in the e-commerce security strategy is found, and the abnormal behavior in the e-commerce environment is dealt with. Resources are integrated and analyzed in a distributed manner, trying to find a safe and stable state of e-commerce data, and design a security defense model for the e-commerce early warning system [11, 12], as shown in Figure 2.

2.2. Concept and Structure of Blockchain.

(1) The version number indicates the version information of the relevant protocol in the blockchain.

(2) *The Hash Value of the Previous Block*. In each block, the hash value of the previous block is marked. The block is connected end to end through this value to form a block chain, which ensures that the transaction time is recorded in the block, become irreversible, and form the security of the blockchain [13, 14].

(3) Timestamp can accurately mark the time when the block is generated in the block, ensuring the uniqueness of the block [15].

(4) Nonce is randomly generated by the system, that is, the answer to the math problem in the block that will be confirmed by the entire network. In essence, the random number mechanism is essential to ensure the decentralization of the blockchain because once the random number is manipulated or predicted, malicious nodes can use this to control the block and achieve double-spending attacks [16, 17].

(5) The Merkle root is the hash value of all transactions recorded in the main body of a block, which is calculated through two-by-two hash calculation. Therefore, the Merkle root is a data structure that can effectively summarize all transactions in a block and is used to index and organize all transaction information in the block [18, 19]. The BcRCACDAM system architecture is shown in Figure 3.

For e-commerce, network security is one of the basic links. Therefore, in order for e-commerce to proceed smoothly, the e-commerce platform must be safe and reliable first, and the services provided must not be interrupted. According to the relevant national standards, when e-commerce is running, actual funding status and information security, the relevant requirements of scientific physical security should be formulated, and then relevant constructions should be adopted to meet the standards. The integrity, confidentiality, and authenticity of e-commerce must be realized; the system's security vulnerabilities should be resolved as soon as possible; through security reinforcement, further use safety technology to protect the equipment, so that the system's security protection capabilities can be strengthened.

3. Relevance Experiment of Big Data Research Platform

3.1. MapReduce Method. MapReduce is a data processing method that uses map and reduce as the main data processing methods. Programmers do not need to understand distributed systems, and they can also use their own programs to perform calculations through distributed systems. When MapReduce is executed, the aap function is first written, and the input key-value pairs are combined into new key-value pairs through various mapping methods. After processing, they are handed over to reduce. Sort out the data with the same characteristic value, then integrate the data according to a certain algorithm, and finally get the output value [20, 21].

$$\text{Map:}\ \ (k, v) \longrightarrow \text{list}(k, v). \tag{1}$$

The logical expression is as follows:

$$\text{reduce:}\ \ (k[i], \text{list}(v[i])) \longrightarrow \text{list}(k', v'). \tag{2}$$

3.2. MapReduce Framework. The MapReduce framework consists of a single main task server and workstations on cluster nodes. The main task server distributes tasks to each workstation and monitors their execution [22, 23]. If it is found that the node is faulty, it is necessary to re-execute the failed task and redesignate a new available node for task assignment through the set backup task data [24, 25].

$$T_1 = T_C + T_D\left(1 - \frac{D}{D_f * B_n}\right). \tag{3}$$

It can be seen that when $B_n = 1$, since $D > D_f$, then $T_1 < T_2$, the block time is greater than the nonblock time. When $B_c \geq D_c$, it has to be divided into blocks.

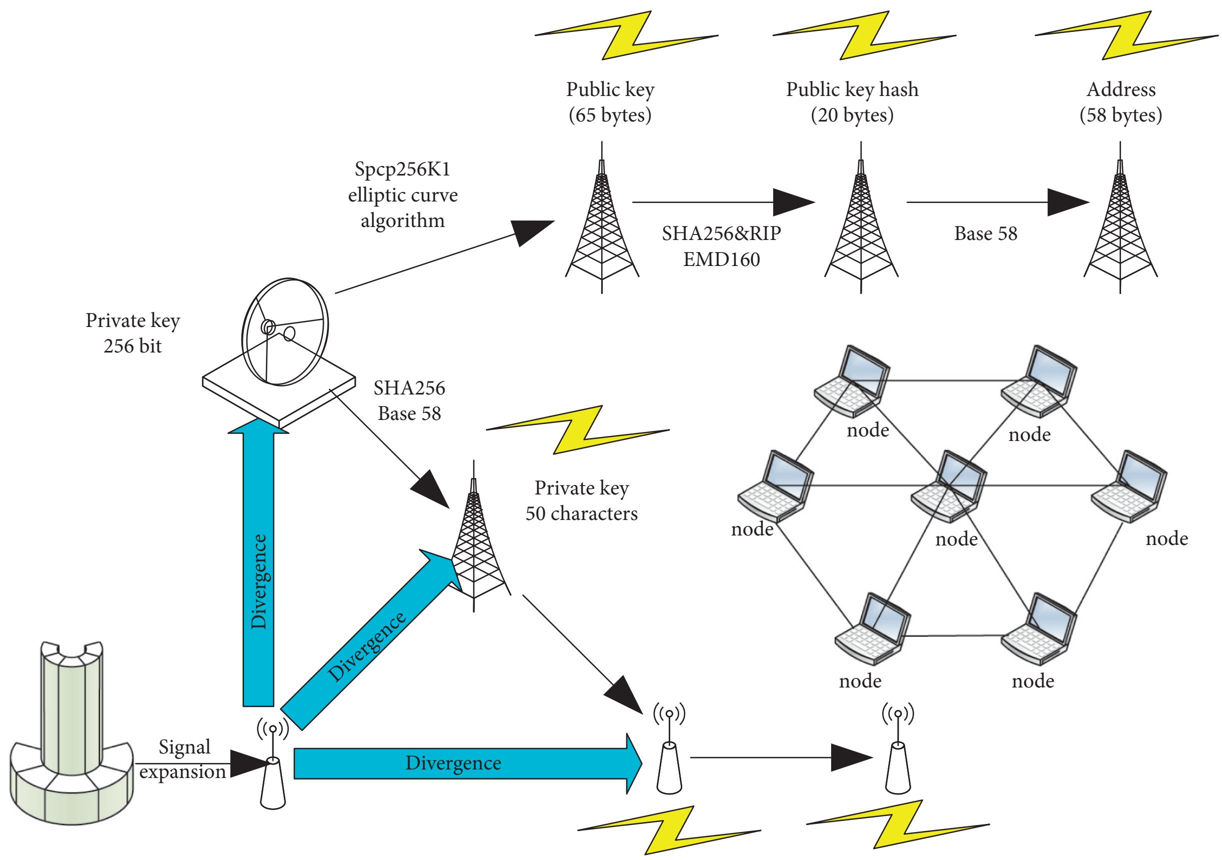

Figure 1: The blockchain asymmetric encryption mechanism.

$$T_1' = T_c + T_D + \frac{D}{D_c}. \quad (4)$$

For the block size setting, the algorithm idea compared with the grouping factor $\{a_0, a_1, \ldots, a_n\}$ is adopted. The specific algorithm is as follows [26, 27]:

$$T_1' - T_2' = T_D\left(1 - \frac{c}{D_c * A_n}\right) + \frac{C}{D_c} - \frac{D}{B_c}. \quad (5)$$

The subject of data ownership refers to the individual or organization that owns the data files and copies, represented by the symbol S; the object of data ownership refers to the data files and copies, represented by the symbol C [28, 29]. Then, according to the characteristics of the subject's access control to the ownership of the object, the object can be further divided into two parts:

$$\forall C_1, C_2 \in C, C_2 = W(S, C_1). \quad (6)$$

According to the above definition and division, the following definitions and rules of data ownership can be obtained [30, 31]:

$$C_1 \in \text{ownby}(S) \cap C_2 = w(t, c_1). \quad (7)$$

Then, t's operation on copy c_1 does not change s' ownership of its object c_1 [32, 33]. Therefore, the data sharing security model can be described as follows:

$$\sum_{i=1}^{k}\left[L_1^*(Z_j) - L_2^*(Z_I)\right]. \quad (8)$$

Least squares is used to determine and calculate the similarity of the sorting sequence and then calculate the difference between the number of characters in the two sorting sequences and then square. The similarity threshold b is an important parameter used to compare the similarity of the watermark with the selected threshold, which has a certain effect [34, 35].

The nodes in the consensus set R_1 participate in the consensus algorithm. Assuming that the maximum number of Byzantine nodes that can be tolerated in R_1 is f, then the size of the set R_1 satisfies the formula as follows:

$$|R_1| \geq 3f + 1. \quad (9)$$

Candidate set R_2 serves as a buffer to receive new nodes added to the system and Byzantine nodes eliminated from the algorithm and provides active nodes for the consensus set. Without loss of generality, we make

$$|R_2| = f. \quad (10)$$

The p value sorted out is as follows:

$$p = (h + v) \bmod |R_1|, \quad (0 \leq p < |R_1|). \quad (11)$$

A consensus proposal is broadcasted for a block to other consensus nodes:

Figure 2: Schematic diagram of blockchain structure (the picture comes from http://www.soxunwang.com/zl/2018/0112/26527.html).

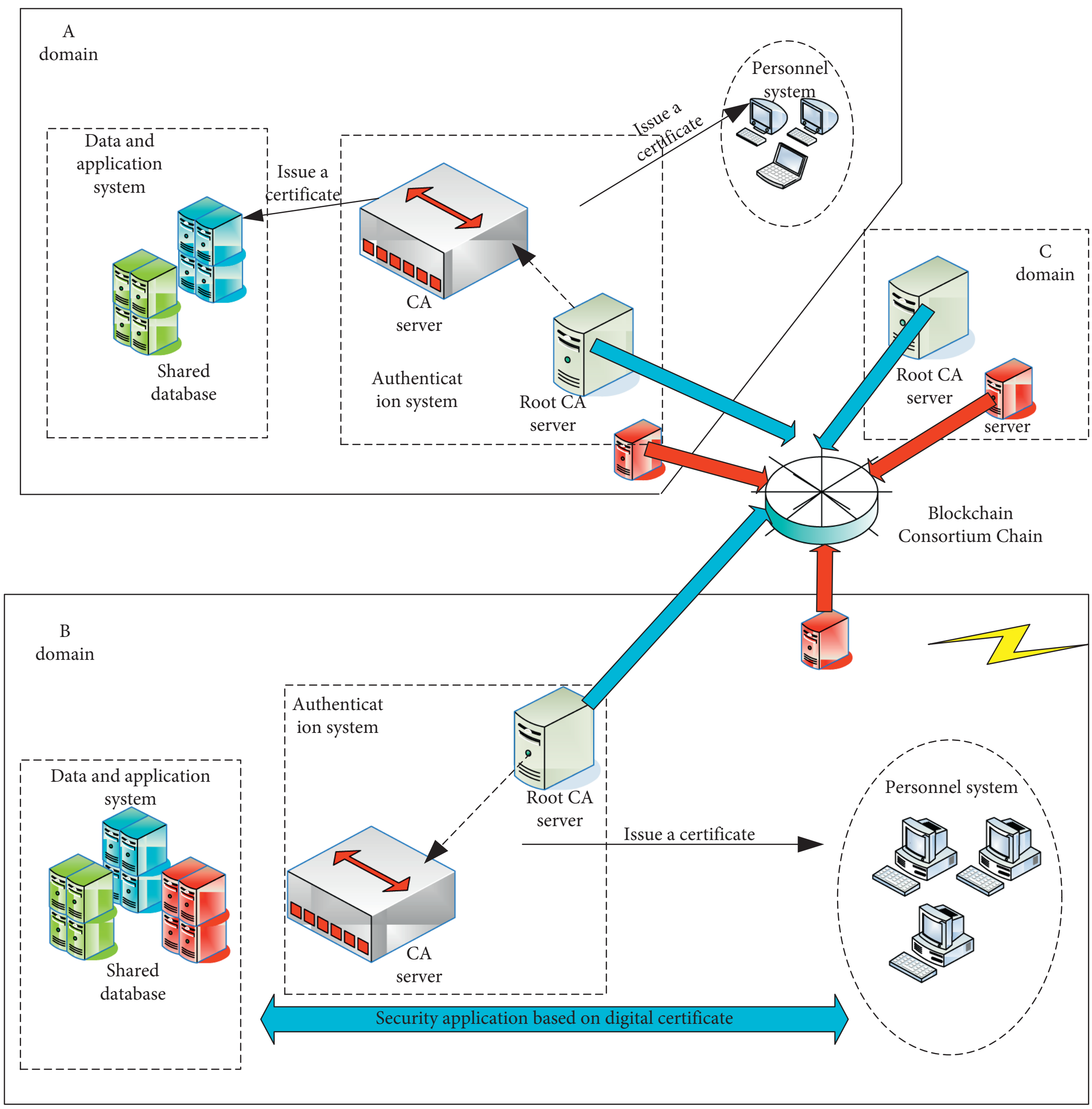

Figure 3: The BcRCACDAM system architecture.

$$\langle \text{Consenus} - \text{Proposal}, \text{view}, h, p, \text{block} \rangle_{\sigma}. \tag{12}$$

A newly elected representative node sends a synchronization request to the nodes of the consensus set as follows:

$$\langle \text{Synchron} - \text{Request}, r_1, h_m, h_n \rangle \sigma. \tag{13}$$

The nodes in the consensus set reply to the representative node with a synchronization message as follows:

$$\langle \text{Synchron} - \text{Replay}, V_{\text{acc}}, r_i \rangle_{\sigma}. \tag{14}$$

Node R_1 broadcasts a view switching request to other nodes:

$$\langle \text{ChangeView}, h, r_i, v, v_k \rangle. \tag{15}$$

4. Electronic Economy Analysis Based on Blockchain

4.1. Leader Node Configuration Analysis. After a follower is successfully elected as the leader node, this role state does not last forever. When the following two situations are encountered, the leader will be replaced: the leader node sends outages such as failures due to network problems and so on. When it can no longer send data to other nodes, it needs to re-elect a new leader; after the leader completes the storage task of the quantitative block, even if there is no failure in the machine, he must return to the role of follower and give up the leadership. One verification node serves as the leader. The node configuration is shown in Table 1.

The client submits data information, such as creating credentials, to the verification node cluster within a specified time such as creating a voucher. As the transaction volume increases, blocks are continuously generated, verified, and stored. The process here guarantees the stability of the algorithm and subsequently provides a template for the International Settlement System process. This basically means one connection and two, and both of them have figured out. Through setting up experimental verification, the results show that the consensus algorithm based on the Raft algorithm proposed in this paper can realize the storage process of transaction data, such as block generation, verification, and leader node replacement, as shown in Table 2.

4.2. Leader Node Security Algorithm and International Settlement Analysis. Due to the consensus algorithm proposed in this article, Raft's leader mechanism is improved. International settlement is also called "international settlement." Through international currency receipts and payments, the claims and debts that occurred between countries due to economic, political, and cultural exchanges were settled. This is closely related to the development of the electronic economy, and the security algorithm can directly reflect the methods of international settlement. The leader role is assumed by all verification nodes in turn. After a leader node completes the storage task, it directly transfers the leadership to the next node. Because there is no election process for leader switching at this time, only data transmission occurs between the leader and the next leader node, and all network overheads are low. The abscissa represents the number of verification nodes, and the ordinate represents the number of verification nodes participating in the leader switching process, as shown in Figure 4.

When the consensus mechanism is running between the verification nodes, a single verification node is tested, and its CPU usage is shown in Figure 4. It can be seen from the figure that the CPU usage of the consensus mechanism for stable operation is less than 50%. The computing power overhead is not high, which meets the performance requirements of the voucher management and control system. It can be proved that the efficiency of international settlement has also been guaranteed. The leader re-election process is shown in Figure 5.

As shown in Figure 5, even if the leader does not experience downtime and other failures, he cannot continue to serve as the leader after completing the block storage task. In the blockchain consensus mechanism based on the Raft algorithm designed in this paper, the verification node clusters jointly participate in the accounting process and take turns owning the accounting rights. From the initial successful election as the leader, the number of blocks stored under the leader's leadership is recorded. When the number of blocks reaches 10,000, the leader node status changes to a follower, and the leadership is delivered to the next verification node. This can prevent a single node from controlling the accounting rights of the ledger and at the same time reduce the number of leader elections and reduce the overhead of the system.

The comparison of the proportion of non-Byzantine nodes between EDA-PBFT and PBFT is shown in Table 3.

Table 4 shows the calculation overhead comparison of BcRCACDAM cross-domain authentication protocol.

BcBICDAM protocol calculation overhead comparison is shown in Table 5.

Major foreign security vulnerability database is shown in Table 6.

Data statistics of major security vulnerability databases at home and abroad are shown in Table 7.

The data volume view of the vulnerability database involved in the system is shown in Figure 6.

Vulnerability and defect type statistics are shown in Figure 7.

The system error rate is shown in Figure 8.

Table 1: Node configuration.

Serial number	IP address	System	Memory capacity (G)	Hard drive capacity
1	192.168.2.136	WIN10	8	256G solid state
2	192.168.1.127	WIN10	8	256G solid state
3	192.168.1.121	WIN10	8	256G solid state
4	192.168.1.125	WIN10	8	256G solid state

Table 2: Functional verification.

Serial number	Name	Validation results
1	Data signature verification	Signature verification succeeded
2	Block generation	Complete block generation
3	Verify new block	Complete verification of the new block
4	Store new blocks	Complete new block generation
5	Leader node switching	Leader node switch successfully

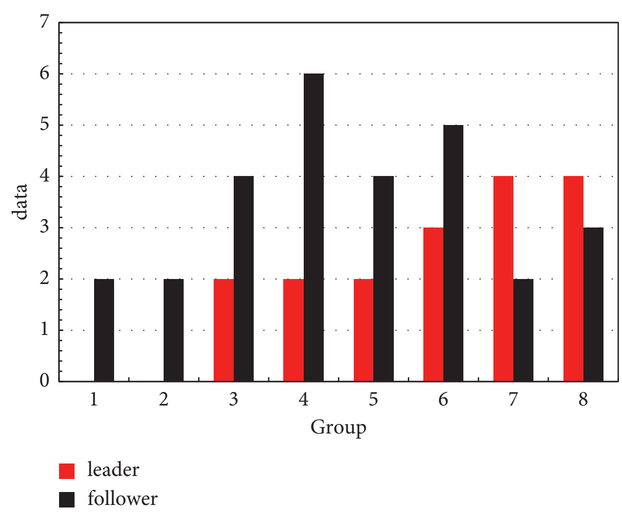

Figure 4: The number of participating nodes in the leader switching process.

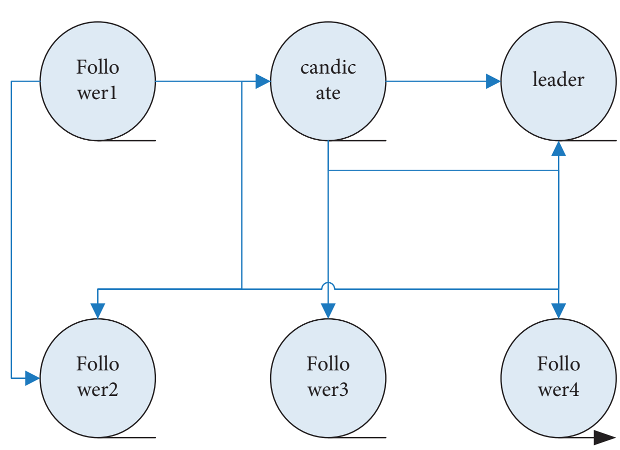

Figure 5: Leader re-election process.

Table 3: The comparison of the proportion of non-Byzantine nodes between EDA-PBFT and PBFT.

Consensus set number of Byzantine nodes	0	1	2	PBFT
0	1	1	1	1
1	1	1	6/7	6/7
2	1	6/7	5/7	5/7

Table 4: Comparison of calculation overhead of BcRCACDAM cross-domain authentication protocol.

Program	Public key encryption and decryption	Digital signature and verification	Hashing
Plan A	2	4	10
Plan B	0	12	14
Plan C	0	4	2

Table 5: BcBICDAM protocol calculation overhead comparison.

Program	Service	Fuzzy extraction operation	Exponential calculation	Hash algorithm	Symmetric encryption/ decryption	Asymmetric encryption/ decryption
Plan A	Terminal	2	2	4	0	0
	Service	0	0	0	0	0
Plan B	Terminal	2	0	10	1	0
	Service	0	0	2	0	0
Plan C	Terminal	2	2	1	1	2
	Service	0	1	1	1	0

Table 6: Major foreign security vulnerability database.

Vulnerability library name	Website address	Abbreviation
National vulnerability database	http://nvd.nist.gov	NVD
BugTraq security focus	http://seclists.org	Bugtraq
Packet storm secutity	https://packetstormsecurity.com	PacketStorm
Exploit-database	https://www.exploit-db.com	Exploit-db
Metasploit vulnerability database	https://www.rapid7.com	Metasploit
Security focus vulnerability database	http://www.securityfocus.com	Secfocus
Cxsecurity vulnerability database	https://cxsecurity.com	Cxseccurity
Oracle Linux errata repository	https://Linux.oracle.com	oracleLER
Ubuntu security notices	https://www.ubuntu.com	ubuntuSN
Microsoft security bulletins	https://technet.microsoft.com	microsoftSB

Table 7: Data statistics of major security vulnerability databases at home and abroad.

Vulnerability library name	Language	Total amount of data	Contains the number of CVEs	Number of fields	Contains vulnerability verification information	Contains patch information
CVE	English	11.16	11.16	9	No	No
NVD	English	9.41	9.41	16	Yes	Yes
Cxsecurity	English	2.38	1.12	18	Yes	No
Exploit-db	English	3.84	2.32	11	Yes	No
Packetstorm	English	9.8	2.59	7	Yes	No
Ubuntu	English	0.4	0.36	9	No	Yes
Secfocus	English	9.19	6.2	16	Yes	Yes
CNVD	Chinese	7.7	4.68	16	No	Yes
CNNVD	Chinese	9.3	8.63	14	No	Yes
SCAP	Chinese	11.16	11.16	9	No	No

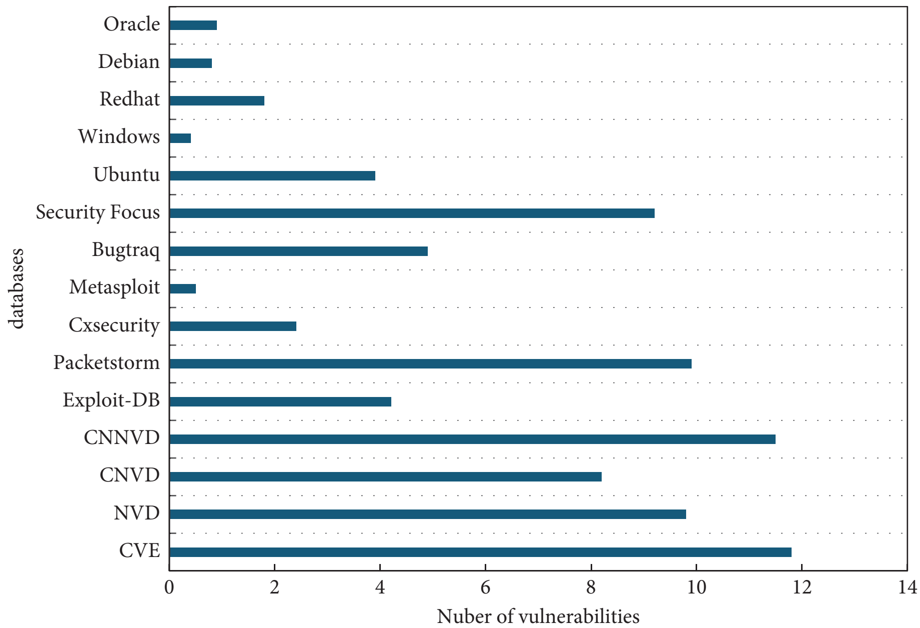

Figure 6: The data volume view of the vulnerability database involved in the system.

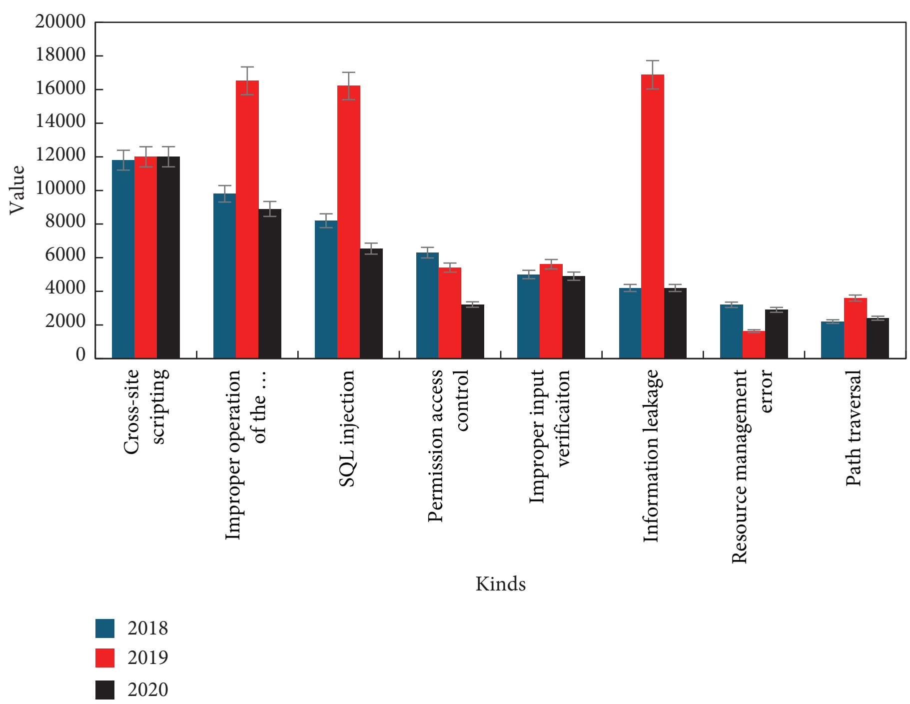

Figure 7: Vulnerability and defect type statistics.

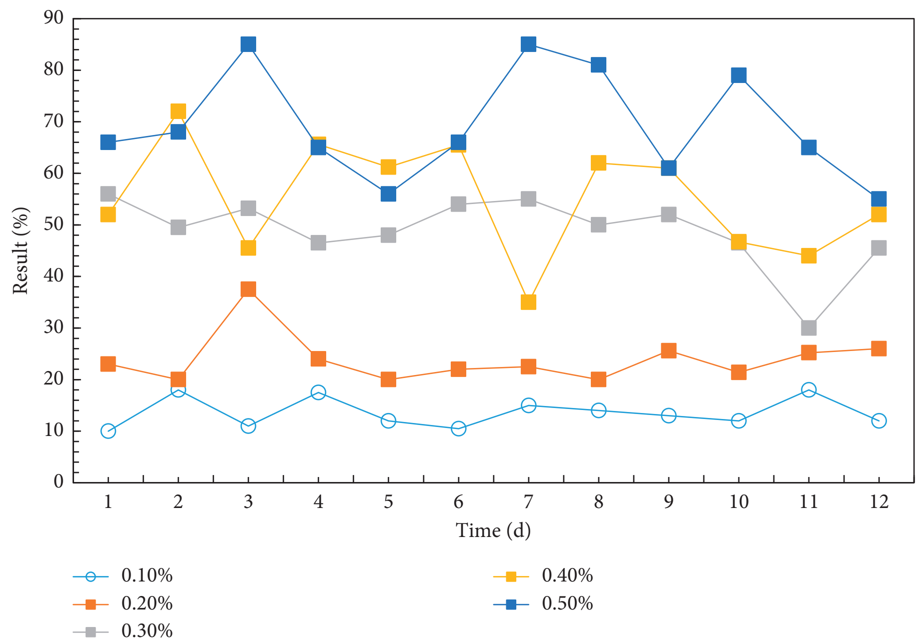

FIGURE 8: The system error rate.

5. Conclusion

On the basis of summarizing the research status at home and abroad, combining with the origin of the development of electronic economy, this paper puts forward the connotation and definition of supply chain finance, summarizes the classification form of supply chain finance, and sorts out the differentiated development of supply chain finance in different historical stages. And it further analyzes the content, motivation, and degree of sharing of the data. Through analysis of security algorithms, international settlement is included. Based on the electronic economy, online settlement methods are also clearer. Experiments have shown that the security of the electronic economy has increased by at least 60%. In the same way, the efficiency of international settlements has also improved accordingly. Finally, this article uses company *D* as a case to introduce the strategy, organizational structure, specific operations, risk prevention, and results achieved by company *D* in developing supply chain finance based on data sharing. The shortcomings of this article are as follows. Due to the limited time, some modules of the system need to be further improved, such as the user key management module. Currently, verification nodes cannot enter the network freely. On the basis of completing the basic functions, performance considerations are insufficient. The system implementation of the voucher management and control system is given, and the safety and effectiveness of the system are evaluated. Evaluation shows that the management and control system can resist most frauds and ensure the security of transaction data. Further research work in the future is as follows: improving various modules of the system, such as user key management and other modules. The peer-to-peer network module needs further research and optimization. On the basis of completing system functions, further performance indicators are improved such as CPU usage, and a more comprehensive experimental process is designed.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest in this study.

References

[1] L. Li and J. Zhang, "Research and analysis of an enterprise E-commerce marketing system under the big data environment," *Journal of Organizational and End User Computing*, vol. 33, no. 6, pp. 1–19, 2021.

[2] G. He, "Enterprise E-commerce marketing system based on big data methods of maintaining social relations in the process of E-commerce environmental commodity," *Journal of Organizational and End User Computing*, vol. 33, no. 6, pp. 1–16, 2021.

[3] P. Wang and W. Han, "Construction of a new financial E-commerce model for small and medium-sized enterprise financing based on multiple linear logistic regression," *Journal of Organizational and End User Computing*, vol. 33, no. 6, pp. 1–18, 2021.

[4] C. Maican, A.-M. Cazan, R. Lixandroiu, L. Dovleac, and M. A. Maican, "Exploring the factors influencing the use of communication and collaboration applications," *Journal of Organizational and End User Computing*, vol. 33, no. 4, pp. 94–124, 2021.

[5] A. N. Khan, X. Cao, and A. H. Pitafi, "Personality traits as predictor of M-payment systems," *Journal of Organizational and End User Computing*, vol. 31, no. 4, pp. 89–110, 2019.

[6] Y. Jin, X. Xu, and G. Wang, “Research on E-government big data security sharing based on blockchain,” *Information Security Research*, vol. 4, no. 11, pp. 1029–1033, 2018.
[7] C. Zhou, “Exploring the safety management of medical big data based on blockchain technology,” *China Collective Economy*, vol. 643, no. 23, pp. 158-159, 2020.
[8] J. Wang, Z. Zheng, and W. Fan, “Data market based on blockchain,” *Big Data*, vol. 6, no. 3, pp. 25–39, 2020.
[9] Z. Pei, “Analysis of the security sharing of E-government big data based on blockchain,” *Electronics Test*, vol. 452, no. 23, pp. 89-90, 2020.
[10] Z. Zeng and P. Wan, “Research on public security big data resource management system based on sovereign blockchain network,” *Information Theory and Practice*, vol. 42, no. 008, pp. 110–115, 2019.
[11] S. Wang, W. Liu, and Y. Wang, “Research on the integrated development of “big data + blockchain” in the sharing economy,” *Journal of Hubei Institute of Adult Education*, vol. 24, no. 6, pp. 87–90, 2018.
[12] T. Cao and Y. Wang, “The key role of ABCD in the smart industry of traditional Chinese medicine and blockchain,” *Frontiers of Chinese Medicine Research*, vol. 2, no. 1, pp. 20–24, 2020.
[13] R. Zhou, H. Liu, and Y. Jin, “Research on the development path and countermeasures of sharing economy based on blockchain technology,” *Guangxi Social Sciences*, vol. 001, no. 002, pp. 84–87, 2018.
[14] Q. Yu and P. Li, “Research on “high-speed railway + shared car” data circulation based on blockchain,” *Railway Transport and Economy*, vol. 41, no. 6, pp. 92–96, 2019.
[15] C. Liang, “Research on the development of sharing economy based on “big data + block chain” technology,” *Marketing: Agricultural Materials and Markets*, vol. 421, no. 20, pp. 180–182, 2019.
[16] G. Wang, “Research on the development of sharing economy based on “big data + blockchain”,” *Business Times*, vol. 010, no. 13, pp. 84–86, 2018.
[17] Y. Zheng, Y. Jiang, and J. Zhou, “Research on industry chain data sharing and circulation based on blockchain technology,” *Modern Marketing*, vol. 041, no. 001, pp. 102-103, 2020.
[18] L. Wang, L. He, and J. Niu, “Blockchain-based geoscience big data management,” *National Defense Technology*, vol. 39, no. 2, pp. 70–78, 2018.
[19] J. Wang, W. Sheng, and K. Dai, “Research on the open sharing system of big data in science and technology finance based on blockchain,” *Modern Computer (Professional Edition)*, vol. 622, no. 22, pp. 54–60, 2018.
[20] Y. Liu and Y. Liu, “RFID big data security traceability model based on blockchain[J],” *Computer Science*, vol. 045, pp. 367-368, 2018.
[21] H. Yang, N. Zhou, and H. Xia, “Research on the meteorological data sharing scheme based on blockchain technology,” *Modern Agricultural Science and Technology*, vol. 030, no. 11, pp. 205–207, 2020.
[22] S. Huang, L. Chen, and B. Fan, “Data security sharing method based on CP-ABE and blockchain,” *Computer System Applications*, vol. 28, no. 11, pp. 83–90, 2019.
[23] Y. Wang, “Development of sharing economy based on “big data blockchain” technology,” *Information Weekly*, vol. 001, no. 52, 2019.
[24] L. Jia, X. Zhou, and X. Bai, “Research on the application of blockchain in government affairs system,” *Cyberspace Security*, vol. 10, no. 11, pp. 19–24, 2019.
[25] L. Tang, “Research on the development of \\“big data + block chain\\” sharing economy based on the theory of industrial integration,” *Operator*, vol. 032, no. 10, pp. 19–33, 2018.
[26] Y. Hu, “Big data + blockchain” sharing economy development research——based on the theory of industrial convergence,” *Enterprise Technology and Development*, vol. 462, no. 4, pp. 20-21, 2020.
[27] S. Zhu, C. Li, R. Huang, and W. Li, “Blockchain-based medical data security sharing model and mechanism,” *Computer Technology and Development*, vol. 30, no. 10, pp. 129–136, 2020.
[28] Y. Song, “Research on sports big data integration and communication innovation based on blockchain,” *Journal of Chengdu Sport University*, vol. 44, no. 6, pp. 65–71, 2018.
[29] C. Cui, “Discussion on the development of basic theoretical issues of auditing boosted by big data-based on blockchain technology,” *Economic System Reform*, vol. 005, no. 003, pp. 85–90, 2018.
[30] X. Ding and X. Su, “Financial security intelligence analysis based on blockchain trusted big data artificial intelligence,” *Journal of Information*, vol. 038, no. 12, pp. 1297–1309, 2019.
[31] H. Yan, “Research on the method of using blockchain technology to construct a data circulation safety supervision system in the process of big data sharing and exchange,” *Information Weekly*, vol. 007, no. 17, 2018.
[32] Y. Yang, “Autonomous driving technology based on big data and blockchain,” *Auto Interiors*, vol. 004, no. 15, pp. 35-36, 2019.
[33] B. Zhang and M. Wang, “A new mode of data sharing based on blockchain technology[J],” *Contemporary Financier*, vol. 005, no. 10, pp. 121–123, 2019.
[34] J. Song, B. Dai, and L. Jiang, “Data governance collaboration method based on blockchain,” *Computer Applications*, vol. 38, no. 9, pp. 58–64, 2018.
[35] X. Chen, Y. Jiang, and L. Jia, “Research on blockchain smart contract technology for big data integration and sharing,” *Information Recording Materials*, vol. 20, no. 10, pp. 161–163, 2019.