Scholar Publishing Group
International Journal of Big Data Intelligent Technology
https://doi.org/10.38007/IJBDIT.2026.070113
ISSN 2790-0932 Vol. 7, Issue 1: 102-113

Blockchain Based Communication Network Security Intrusion Detection Data

Ziyi Huang

School of Public Security Information Technology and Intelligence, China Criminal Police University, Shenyang, Liaoning, China

Keywords: Blockchain Technology, Communication Network, Intrusion Detection, Consensus Mechanism

Abstract: Communication network security not only continuously provides convenience for humans, but also creates security risks due to the open and intelligent nature of the network. The purpose of this article is to use blockchain technology (BCT for short here) to solve the problem of communication network security being invaded, and analyze this for network security on the blockchain through consensus mechanisms. After introducing the methods of consensus mechanisms such as Proof of Work (POW), Proof of Stake (POS), and PBFT (Practical Byzantine Fault Tolerance), this article mainly conducted experimental discussions on the PBFT consensus mechanism. Finally, this article concluded that comparing PBFT with TBFT (Tencent Byzantine Fault Tolerance), the improvement space of TBFT still needs to be improved. After the methods of these consensus mechanisms, experimental analysis was mainly conducted for the PBFT consensus mechanism. The average time for generating experiments was 0.027 ms, and the average time for verifying experiments was 0.002 ms. Finally, it can be concluded that comparing PBFT with TBFT in this article, the improvement space of PBFT still needs to be improved.

1. Introduction

In recent years, the application technology of blockchain has become more and more widespread. Many experts in the research field of blockchain have extended their analysis of this technology, citing its methods in various industries, shopping malls, markets, or government agencies. Blockchain, as one of the operations required for future development, not only can transmit value, but also allow users to master their own data and have a comfortable operating system. Blockchain is also a system for network security, mainly measures taken to prevent information from being used, modified, or destroyed without authorization. Network security also requires ensuring that information systems can operate continuously, reliably, and normally. Due to the different characteristics between BCT and Internet technology, Belchior R has also conducted a comprehensive survey of the development, architecture, development framework, and security issues of BCT. He also conducted a comparative analysis of the frameworks used in blockchain, the

classification of consensus algorithms, and security risks and passwords. He also elaborated on the main directions and challenges of blockchain in the future for future researchers to explore [1]. Based on how blockchain is used in business, Morkunas V J provided an introduction to BCT for general managers and executives. His main contribution was to provide an explanation of blockchain, including blockchain trading work and terminology clarification, as well as an overview of different types of blockchain technologies [2].

In the face of network intrusion, network security, and information leakage, scholars have conducted a large amount of research. By evaluating existing defense technologies, they have classified the security threats and challenges of the Internet of Things (IoT) network. In order to identify, prevent, or detect new types of attacks, it is important for Chaabouni N to analyze the technology in the IoT environment. The focus is on the Network Intrusion Detection System (NIDS). Therefore, he reviewed existing NIDS implementation tools and datasets, as well as free and open source network sniffing software. He investigated, analyzed, and compared the most advanced NIDS recommendations in the IoT environment in terms of architecture, detection methods, verification strategies, processed threats, and algorithm deployment. He discussed the traditional machine learning (ML) NIDS technology, focusing on the IoT NIDS deployed through ML, because learning algorithms have a good success rate in security and privacy. Unlike other top-level surveys of traditional systems, he mainly considers the limitations of the IoT, and therefore proposes new intelligent technologies in the context of the IoT [3]. When traditional conventional intrusion detection rules and secure network systems can no longer meet the ever-changing and timely intrusion prevention requirements. Wang H found that with the rapid development of network technology, network security is increasingly receiving attention from researchers in various fields. Therefore, he proposed an intrusion detection method based on Convolutional Neural Network (CNN). On this basis, he designed an efficient, real-time, and automated intrusion detection system: Intrusion Detection System—Convolutional Neural Network (IDS CNN). The system is built by multiple open source tools, such as the packet capture interface Tcpdump, the traffic analysis interface BRO, and the machine learning interface Tensor flow. The system is based on Linux platform and consists of data preprocessing, neural network training, network testing, and intrusion response [4].

Because BCT provides distributed ledgers, this technology alone cannot provide network security. Therefore, Sedlmeir J conducted a comprehensive review of blockchain distributed ledgers and analyzed the technologies and elements of BCT in achieving network security. Finally, he believed that blockchain can provide security for communication networks to a certain extent [5]. Taylor P J identified peer reviewed literature seeking to use blockchain for network security purposes, and conducted a systematic analysis of the most commonly used blockchain security applications. Finally, he found that the IoT was very suitable for new blockchain applications. The visualization of networks and machines, public key cryptography, web applications, authentication schemes, and secure storage of personal identity information were also suitable for application in blockchains [6].

In terms of BCT, it may be considered a key turning point for organizational cooperation. By understanding the historical background and basic characteristics of blockchain, scholars have analyzed the role of governance mechanisms. It is believed that blockchain provides a way to implement agreements and achieve cooperation and coordination, which is different from traditional contract and relationship governance as well as other information technology solutions. Under current environmental conditions, people attach great importance to the social impact of blockchains, as well as their inherent challenges and limitations. Therefore, this article discusses and analyzes blockchains based on communication network security.

2. Blockchain under Communication Network Security

2.1 Blockchain

Blockchain is essentially a decentralized database, a new application model for computer technology such as distributed data storage, point-to-point transmission, protocol processing, and encryption algorithms. This technology integrates professional technologies in various fields such as mathematics, networking, cryptography, and computer programming. Blockchain is a distributed shared database that is connected in chronological order and forms a tamperproof digital structure.

The advantages of blockchain include: decentralization, no centralized management mechanism, all nodes have equal power, and any error at any one node would not affect the entire system. Decentralization is the most prominent feature of blockchain. Information is not tamperable. When information is added to the blockchain, it would always be blocked, and modifications to a node would be invalid. The data in the blockchain is very reliable. Openness: All data in the blockchain is open to anyone, anyone can query data through an open interface, and can access the entire system very transparently [7].

The disadvantages of blockchain are as follows. Security issues: accounts used by individuals are easily stolen; Data validation takes a long time. Lately restricted: The decentralized and self-disciplined nature of blockchain weakens the concept of restriction, and regulatory authorities lag behind in their legal system for this technology.

This article also compares blockchain with traditional databases, as shown in Table 1.

Table 1 Differences between blockchain and traditional databases

Blockchain	Traditional database
There is no administrator/central organization	By the administrator/central organization
No one can control all the nodes	Records in the database can be modified and managed
Decentralized, distributed network architecture	Centralized database
Information openness and transparency	You can set access permissions

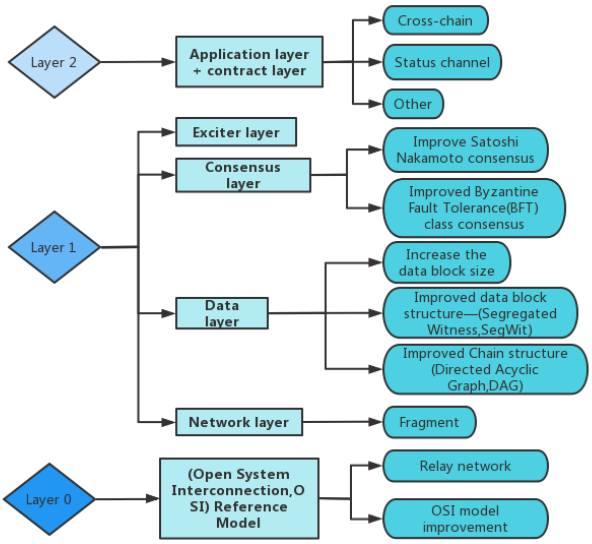


Figure 1 Blockchain Layered Architecture Diagram

The entire network of a personal chain is managed by an organization that has full authority to allow anyone to participate in the maintenance of the blockchain network. A federated chain is a blockchain of institutional alliances, and access and authoring permissions are only open to nodes that join the organizational alliance.

Blockchain is a distributed system. Figure 1 shows the architecture of blockchain.

2.2 Communication Security Intrusion Detection

Intrusion detection system refers to testing the main functions of software in the role of a user. The general inspection methods include feature inspection, statistical inspection, and expert system. The types of system testing include functional testing, performance testing, safety testing, and compatibility testing. Feature detection provides a definitive explanation of known attacks or intrusion patterns, forming corresponding event patterns. This method has high accuracy in prediction and measurement, but it is powerless for intrusions and attacks without empirical knowledge. Statistical models typically perform exception detection, and the variables typically measured by statistical models include the number of audit events, time intervals, resource consumption, and so on. The five statistical models commonly used for intrusion detection are operational models, which can compare measurement results with fixed indicators to derive the above assumptions. Fixed indicators can be obtained based on empirical values or statistical averages over a given period. The variance model calculates the variance of parameters, with all elements of the design matrix X being 0 or 1. The model parameters are effect values at the factor level, and meet certain linear constraints. The extension of multidimensional model and operation model can analyze multiple parameters simultaneously to achieve detection. The Markov process model defines all types of events as system states, and uses state transition matrices to represent state changes. The time series analysis model ranks the number of events and resource consumption in chronological order. If the probability of a new event occurring at that time is low, the event may be an intrusion behavior [8].

The biggest advantage of statistical methods is that they can learn from users' usage habits and have a high detection rate and availability. This learning ability also allows intruders to gradually train and make intrusion events conform to the statistical rules of normal operation, thereby obtaining the opportunity to intrude through intrusion detection systems.

Advantages of file integrity checking systems: From a mathematical analysis, conquering a file integrity checking system is impossible in both time and space. The file integrity check system is a powerful tool for detecting modified files. In fact, file integrity checking systems are one of the most important tools for detecting whether a system has been illegally used. The file integrity check system is very flexible and can be set to all files or some important files of the display system. When an intruder attacks a system, he does two things. The first is to hide traces. That is, it can hide activities by changing the executable, library, and log files of the system. In addition, there are some changes that can be made to re invade. Both activities can be detected by the file integrity checking system. The weakness of the file integrity checking system is its reliance on a local summary database. Like log files, these data can also be modified by intruders. The intruder obtains the privileges of the administrator and can perform a file integrity check after completing the destruction activity, deceiving the system administrator to confirm that the system is updating the database. Of course, summary databases can also be placed on read-only media, but this structure is not very flexible [9].

Functional testing refers to using test objects to verify whether users meet hidden requirements under the conditions of use. It is necessary to check for incorrect or missing areas and observe whether its functional output is correct. Performance testing mainly refers to verifying whether the

tested object meets its own set goals through the operating pressure of the tested object; Security testing mainly focuses on whether the protection system of the tested object can accept correct infringement operations. Compatibility testing is mainly to verify how the tested object operates in different operating systems, hardware information, and other environments. In recent years, there have been many problems with data leakage. Table 2 lists some cases of privacy leakage.

Table 2 Privacy disclosure cases

Serial number	Event	Influence
1	Facebook Data breach	29 Million user data stolen
2	Cathay Pacific data breach	9.4 Million passengers were affected
3	Yto Express information leaked	A billion user data has been compromised
4	Estee Lauder records leaked	More than 440 million internal records were exposed
5	Exactis Big Data company leaked private information	The privacy of 230 million people was exposed

2.3 Blockchain in Communication Network Security

Currently, the issues of network privacy disclosure and data sales are very serious. These problems exist in both the internet industry and startups. Blockchain is positioned as a low-level public chain platform that supports online chains for any business and can solve issues such as personal information protection and communication costs in the communication industry.

Firstly, blockchain mainly uses asymmetric encryption algorithms to encrypt information to protect user privacy. Asymmetric encryption is safer than symmetric encryption because it does not require the sharing of keys between the client and server. Even if the public key is eavesdropped on the network, data would not be disclosed unless the private key is transmitted to others. Secondly, a blockchain based social platform can bring value to the data and content produced by users, and cultural information can be seen anywhere in the world. Cultural information creators can also obtain corresponding benefits.

After the advent of BCT, users' personal data can be connected to their personal digital identity cards. Users can choose an anonymous or public digital ID card, access the blockchain application platform on any device at any time, and control network personal data. For example, the ID card number, or a series of passwords converted in the facial photo blockchain, is only applicable to the comparison of serial passwords and passwords through the information on the blockchain and the comparison of data results when registering in hotels or some websites. If the data does not match, the data information cannot be viewed. This is a very effective method of protecting personal information. At the same time, developing big data and artificial intelligence (AI) requires a large amount of data resources for users, who can selectively sell their data as cryptocurrency and obtain revenue. In this mode, the platform transfers a portion of the advertising revenue to users, who can decide whether to sell their data at their own discretion. This is a situation where advertising companies, platforms, and users all win. In a centralized world, communication applications are controlled by a centralized operating mechanism, which can easily lead to information leakage. If communication applications are combined with blockchains, the privacy and tamper-proof characteristics of blockchains can ensure that data and information are held in the user's own hands, allowing users to truly have the right to use the data. At the same time, there are currently obstacles between communication application fields, and communication between different application fields is not possible [10].

3. Consensus Mechanism

The consensus mechanism is only intended to achieve one point, that is, under the premise of decentralized web3.0, to ensure the stability, reliability, and authenticity of the system through multi-party authentication methods. The common workload proof mechanism is obvious for the waste of energy. In a blockchain, data is stored and bound together in a chain manner for the purpose of being tamperproof. Unlike centralized architectures, all participating nodes in the blockchain have equal rights to record data. Generally speaking, consensus means that everyone reaches an agreement through negotiation. In a centralized architecture, there is an authority that everyone else listens to. However, due to the decentralized mechanism of blockchain, how to make each node maintain the consistency of their data through a rule is a crucial issue. The solution to this problem is to develop a series of protocol algorithms to achieve consistency and accuracy of account book data on different account book nodes [11].

In short, the consensus mechanism has two functions: 1 Verify the data to ensure its correctness. 2. Filter out a node through consensus mechanism to write data to the chain. Due to the cost incurred by nodes in processing data, most public chains encourage more people to participate through the issuance of digital currency. Currently, common blockchain consensus mechanisms include: Proof of Work (POW), Proof of Stake (POS), and Practical Byzantine Fault Tolerance (PBFT).

3.1 Workload Proof Mechanism

In the POW consensus, this article selects a node through computational power competition, and the node determines the block content of the next round of consensus. In each round of consensus, only one node has a large workload. For example, Bitcoin uses a protocol based algorithm called POW. POW is the measure of the system that achieves a certain goal. In short, it is evidence of how much has been done. The entire process of monitoring work is usually inefficient, but certification of work results to prove that the corresponding workload has been completed is a very efficient way. POW is a distribution based on work. A node is selected through a computational effort competition, which determines the block content for the next round of consensus. In each round of consensus, only one node's workload is effective [12]. The main technique for workload proof is the hash function, whose solution is:

$$\text{Hash}(X) <= \text{Pow\_Target} \tag{1}$$

X is the unknown number of the required solution, Pow_ Target is the target value. The basic idea of constructing a hash function through binary equations is as follows: It can use the hash value of the previous block and the nonce of the current block as the seed number seed, and generate a set of random multivariate quadratic equations over a finite field through a pseudorandom number sequence generator. It can solve a random multivariate quadratic equation system, obtain the solution X, calculate the SHA256 hash value of X, and see if it is smaller than the target value Pow of POW_ Target. If it is less than Pow_Target, it stops. If it is greater than Pow_Target, people need to exhaust Nonce and repeat the above process until the conditions are met. The POW workload proof process can be shown in Figure 2.

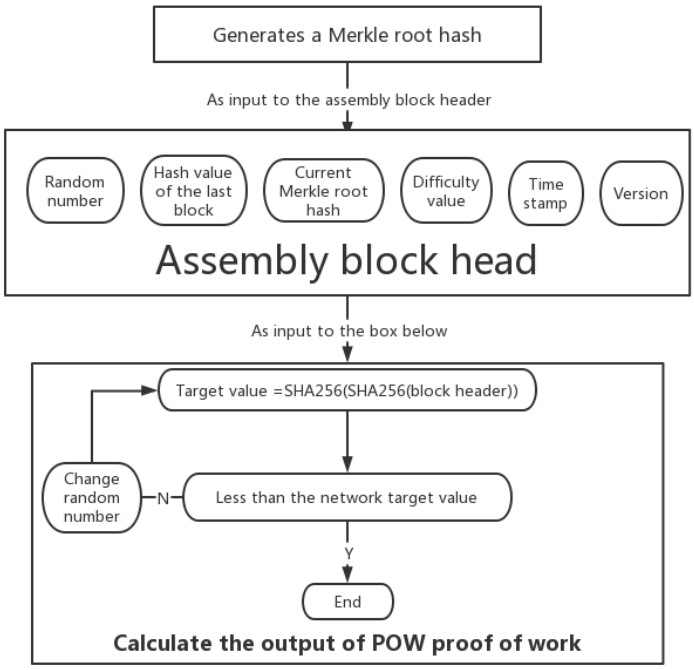


Figure 2 Flow Chart of POW Work Certification

3.2 Proof of Rights and Interests Mechanism

The proof of equity system refers to owning more and more stocks and receiving more rewards. The stock here refers to the amount and time of digital currency held. The more money people hold, the longer they hold it. That is, the older the currency age (currency age=number of currencies people hold * time they hold), the more dividends people would receive. There is also greater accounting power. This mechanism consumes less energy, and the cost of doing evil is high. Its time to reach consensus is short, its currency holdings tend to be centralized, and its liquidity becomes poor. Due to the large amount of energy consumption related to POW, the emergence of POS would solve the following problem: the security of currency using POS is directly related to users, eliminating the medium of miners.

In simple terms, POS is not about the cost of proof every time a news release is released, but rather the cost of proof. "Money" means that if people cheat and disrupt system security, the value of money would decrease and a price would be paid. If POS is used, there is no need to provide external compensation in the actual process. Because POS itself does not need to pay any price.

3.3 PBFT Consensus Algorithm

Compared to POW, PBFT consensus algorithm is more suitable for alliance chains. In alliance chains and even public chain environments, there may be a small number of nodes who, for their own benefit, engage in behaviors that disrupt the consensus of the entire blockchain network. At this point, the consensus algorithm not only needs to consider maintaining the consistency of the blockchain network, but also needs to solve the Byzantine Generals Problem [13].

PBFT is a replica replication algorithm for a state machine. All replicas are operated by view loops, and the primary node is determined by the set of view numbers and node numbers, namely:

$$p = v \bmod |R| \tag{2}$$

v: View number, | R | Number of nodes, p: Master node number. The PBFT consensus flowchart is shown in Figure 3.

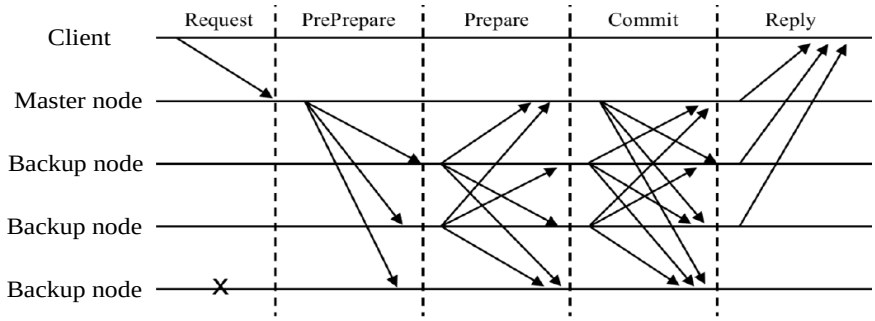


Figure 3 PBFT Identification Flow Chart

To ensure activity, PBFT needs to meet the following requirements:

$$Quorum \le n - f \tag{3}$$

To ensure security, PBFT needs to meet the following requirements:

$$2 * Quorum - n > f \tag{4}$$

Combining the above formula, it is found that PBFT provides a fault tolerance rate of (n-1)/3.

$$n + f < 2 * Quorum \le 2(n - f) \tag{5}$$

4. Results of Practical Byzantine Fault-Tolerant Algorithm

4.1 Communication

In the PBFT consensus algorithm, the client sends an operation request to the master node. PrePrePare sends the original message m, allowing each node to obtain the original message. The master node participates in assigning a unique number to the request, and groups the request and X together to generate a PrepPrePar message, which is broadcast to all members. In the PrePare and Commit stages, when PerPar receives a PrepPrePar message, it mainly relies on the signature segment to check whether the message comes from the primary node. After confirming that there is no error, it broadcasts the message to other members, indicating that it is ready [14].

The node needs to make a decision within 2f+1 state replication communication, which just ensures consistency, but other bad situations can occur. "people can receive f from normal nodes, and f from malicious nodes. At this time, only 2f+1 may be sent normally.". Since the maximum number of malicious nodes is limited, it can be concluded that the requirements of 2f+1 parameters and n>3f+1 are mutually exclusive. That is, each node needs to receive at least 2f messages from other nodes before entering the next stage. However, the client needs to accept at least f+1 Reply messages to determine whether the consensus result is correct [15].

Therefore, if it goes smoothly, a node receiving 1 PrePrePare message and 2f PrePare messages enters the Commit phase, and 2f+1 Commit messages can be replied to the client. Upon receiving f+1 replies, the client can confirm that the submission was successful. Therefore, the client sends an operation request to the master node to determine whether the request has reached a consensus. PBFT requires at least $12f^2 + 7f + 2 \Rightarrow \frac{4}{3}n^2 - \frac{1}{3}n + 1$ communications. If PrePared (m, v, n, i) is

true, then PrePared (m, v, n, j) must be incorrect, because it is impossible to have two results for the same proposal, thereby ensuring the consistency of the entire system. Assuming that the primary node is malicious, it means that there are more than f-1 malicious nodes in the Reply point, and prepared (m, v, n, i) is true. This proves that there are f+1 malicious nodes that have reached a consensus, and prepared (m, v, n, j) is true. This means that another f+1 bona fide nodes have reached an agreement, as there are only 2f+1 bona fide nodes in the system, so at least — bona fide nodes have sent two conflicting PrePare messages, which is impossible. So prepared (m, v, n, i) is true, then prepared (m, v, n, j) is incorrect. The biggest difference between TBFT and PBFT is that PBFT has a fixed leader node to package transactions. When a leader node fails, the view change sub protocol is used to replace the leader; In TBFT, the leaders are rotated, and each time n blocks are submitted (configurable), the leaders are rotated to the next node. Therefore, TBFT has better fairness than PBFT. Comparing PBFT with TBFT, it would be found that TBFT only requires $15f+4 \Rightarrow 5n-1$ communications. In an ideal state, the number of communications required for TBFT and PBFT to conduct a round of consensus is shown in Figure 4.

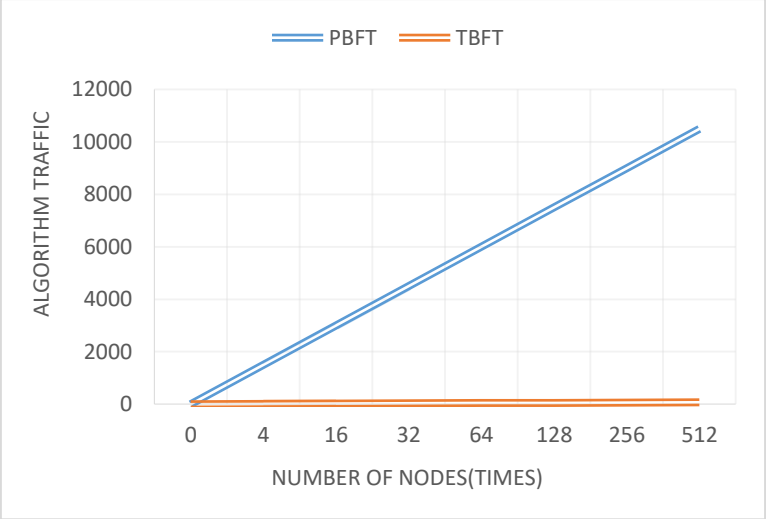


Figure 4 Comparison of communication times

According to Figure 4, it can be seen that with the increase in the number of nodes, the communication frequency of PBFT also shows an upward trend, while the communication frequency of TBFT does not show the same upward trend as that of PBFT. From the processing process, it can be seen that the communication cost of PBFT and TBFT is lower compared to that of TBFT.

From the perspective of consensus algorithm process, through threshold signature, it can be found that TBFT nodes do not need to wait for 2f messages from other nodes. Through Merkel number, TBFT nodes also do not need to wait for f+1 messages from other nodes to obtain consensus. In order to determine whether TBFT has scalability performance in threshold signature and Merkel number, this test was conducted. The test results are shown in Table 3 to Table 4.

Table 3 Threshold signature performance test results

Function	Number of tests	Total time (ms)	Average time spent (ms)
Generate signature	800	1056.735	1.321
Collective signature	150000	682.459	0.005
Verification signature	100	856.347	8.563

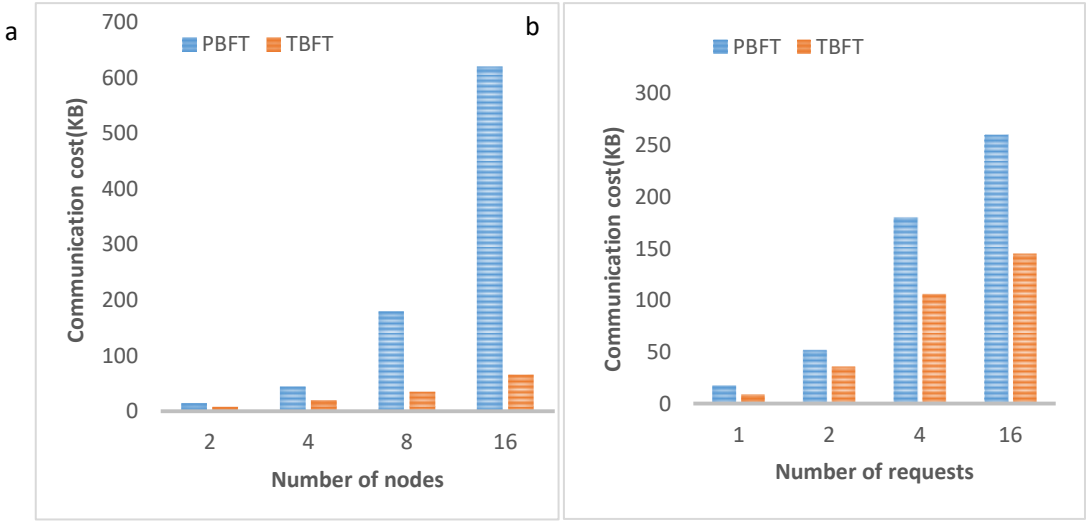
As can be seen from the three functions in Table 3, the average time consumption of the three functions is within 10ms, and the numerical value is 1.321ms for signature generation; The aggregate signature is 0.005ms; The verification signature is 8.563 ms, which is the longest time-consuming signature. The performance test results of Merkel number are shown in Table 4.

Table 4 Merkel number performance test results

Function	Number of tests	Total time(ms)	Average time(ms)
Generate experiment	240000	6521.893	0.027
Verification experiment	450000	598.128	0.001

From Table 4, it can be seen that the average time spent generating and verifying a certificate is within 0.1ms. Combining the results of the two tables, it can be concluded that the Merkel number has a smaller impact on TBFT. Because the average time spent on threshold signature is within 10ms and the average time spent on Merkel number is within 0.1ms.

Based on the test results in Table 3 and Table 4, it can be seen that the verification signature in the threshold signature would have an impact on TBFT. Because the average time spent verifying signatures among threshold signatures is the highest, at 8.563ms, this also means that more time is invested in verifying signatures, and TBFT can have higher throughput. Combined with the above communication cost analysis, TBFT can achieve consensus with a small number of communication times under the same number of nodes. It can be analyzed that TBFT has higher scalability. Here, it can compare the number of information between the two, using the number and size of blockchain requests as the communication cost. Therefore, this article conducts a communication analysis of TBFT/PBFT to determine a consensus communication cost under different node counts, as shown in Figure 5 (a). The communication cost of consensus with different requests on four nodes is shown in Figure 5 (b).



(a) Communication cost under the number of nodes (b) Communication cost under the number of requests

Figure 5 PBFT/TBFT Communication Cost Comparison

As can be seen from Figure 5, as the number of nodes increases, the communication cost difference between PBFT and TBFT becomes increasingly large. Under different requests, it can also be seen that there is a gap between the two, and it can be concluded that the communication

cost of TBFT is lower.

4.2 Throughput

Throughput analysis is also an important indicator of network performance, which refers to the number of transactions that can be processed per second. Throughput in the blockchain, the ratio of transaction value K of throughput to transaction processing time is:

$$T_{PS} = \frac{K}{t} \tag{6}$$

The indicators of throughput include response time, server accessories and facilities, and network status. It can be understood that the greater the throughput, the longer the response time, and the better the accessory facilities of the server, the higher the throughput. A comparison of PBFT/TBFT is shown in Figure 6.

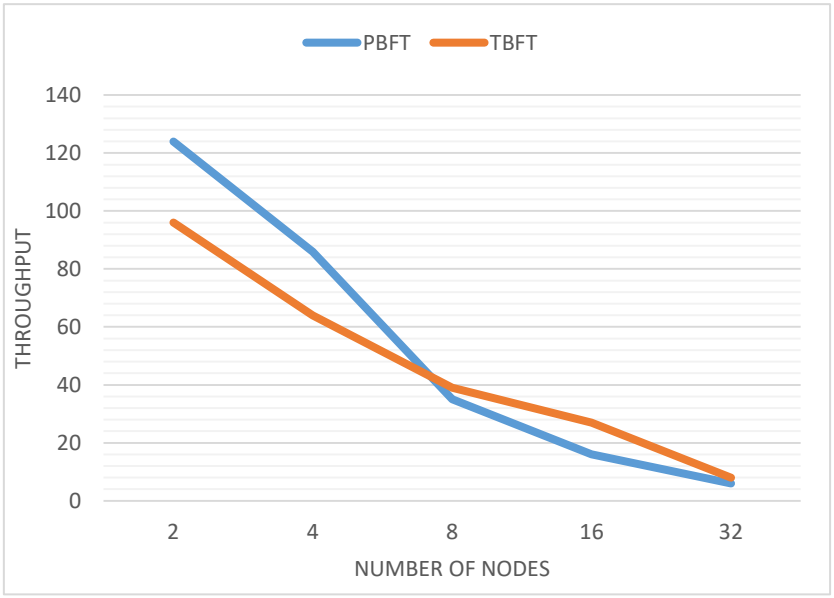


Figure 6 PBFT/TBFT throughput comparison

As can be seen in Figure 6, the throughput of PBFT is higher than that of TBFT before node 7 or so, but after node 7, the throughput of PBFT gradually starts to be smaller than that of TBFT. From Figure 6, it can be concluded that as the number of nodes increases, the throughput of TBFT would be higher than that of PBFT.

4.3 Discussion of Experimental Results

This chapter conducts research and analysis on PBFT and TBFT, and this article analyzes the communication cost and throughput between them. In the communication cost analysis, it is known that the scalability of PBFT is better than that of TBFT. However, compared with Merkel's number later, it can be seen that a large amount of data is more biased towards TBFT, and the method of PBFT needs to be further optimized. In the throughput analysis, it can also be seen that the throughput of TBFT is lower than that of PBFT. Therefore, it is concluded that the TBFT method would continue to be optimized, and there is still room for improvement in this consensus method.

5. Conclusions

Blockchain is a decentralized database that combines technologies such as point-to-point and consensus algorithms. This article conducts research and discussion on blockchain through reference to a large number of documents. In the end, this article would focus on consensus algorithms for blockchain, including workload proof, entitlement mechanism proof, and practical Byzantine fault-tolerance methods based on consensus algorithms, and analyze their advantages, disadvantages, and practicality. In the end of this article, it conducted data experimental analysis on practical Byzantine fault-tolerance, and implemented an extensible optimization scheme for the practical Byzantine fault-tolerance consensus algorithm. Consensus algorithm is a core element of blockchain and a hot algorithm based on blockchain in recent years. However, due to the lack of specific systematic steps for algorithms in this direction, this article has not conducted a more in-depth discussion of practical Byzantine fault-tolerant consensus algorithms, which still requires more references and further improvement.

References

[1] *Belchior R, Vasconcelos A, Guerreiro S. A survey on blockchain interoperability: Past, present, and future trends. ACM Computing Surveys (CSUR), 2021, 54(8): 1-41.*

[2] *Morkunas V J, Paschen J, Boon E. How blockchain technologies impact your business model. Business Horizons, 2019, 62(3): 295-306.*

[3] *Chaabouni N, Mosbah M, Zemmari A. Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, 2019, 21(3): 2671-2701.*

[4] *Wang H, Cao Z, Hong B. A network intrusion detection system based on convolutional neural network. Journal of Intelligent & Fuzzy Systems, 2020, 38(6): 7623-7637.*

[5] *Sedlmeir J, Buhl H U, Fridgen G. The energy consumption of blockchain technology: Beyond myth. Business & Information Systems Engineering, 2020, 62(6): 599-608.*

[6] *Taylor P J, Dargahi T, Dehghantanha A. A systematic literature review of blockchain cyber security. Digital Communications and Networks, 2020, 6(2): 147-156.*

[7] *Bhaskar P, Tiwari C K, Joshi A. Blockchain in education management: present and future applications. Interactive Technology and Smart Education, 2021, 18(1): 1-17.*

[8] *Haislip J, Lim J H, Pinsker R. The impact of executives' IT expertise on reported data security breaches. Information Systems Research, 2021, 32(2): 318-334.*

[9] *Shen M, Tang X, Zhu L. Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. IEEE Internet of Things Journal, 2019, 6(5): 7702-7712.*

[10] *Zhang J. Interaction design research based on large data rule mining and blockchain communication technology. Soft Computing, 2020, 24(21): 16593-16604.*

[11] *Huang J, Kong L, Chen G. Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3680-3689.*

[12] *Cao B, Zhang Z, Feng D. Performance analysis and comparison of PoW, PoS and DAG based blockchains. Digital Communications and Networks, 2020, 6(4): 480-485.*

[13] *Gao S, Yu T, Zhu J. T-PBFT: An EigenTrust-based practical Byzantine fault tolerance consensus algorithm. China Communications, 2019, 16(12): 111-123.*

[14] *Yao H, Mai T, Wang J. Resource trading in blockchain-based industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3602-3609.*

[15] *Yoo S. A study on consensus algorithm based on Blockchain. The Journal of The Institute of Internet, Broadcasting and Communication, 2019, 19(3): 25-32.*