Optimization of PBFT Algorithm in Cloud Environment and Its Application in Logistics Blockchain Consensus Algorithm

Yetong Xi[a] and Ying Liu[b*]

College of Chemistry and Environment, Geely University of China, Chengdu 641423, Sichuan, China
[a]xiyetong@bgu.edu.cn
[b]s_liuying@bgu.edu.cn
**Corresponding Author*

Abstract: *With the rapid development of e-commerce, the logistics industry has also developed rapidly. However, at present, the service transaction system of the logistics industry is highly centralized, the coordination ability is poor, and the customer information security cannot be effectively guaranteed, which affects the information security, automation, and intelligence of logistics enterprise service transactions. The purpose of this article is to study the consensus algorithm of logistics blockchain based on cloud computing. Based on the basic principles of the practical Byzantine consensus algorithm and the logistics blockchain cloud computing model, combined with decentralization and non-repudiation of information security theory, this paper proposes a cloud computing-based logistics blockchain consensus algorithm. Parallel processing functions for design and algorithm analysis. The experimental results show that the test indicators of the algorithm are better than the practical Byzantine consensus algorithm and the optimized MinBFT algorithm. Therefore, this algorithm is an effective blockchain consensus algorithm in logistics service transactions. It has certain application to the logistics industry. Practical significance. In this paper, by testing the security of the algorithm, it is obtained that the attack success rate is 0 when the number of forged nodes differs from normal nodes by 20, and it can be seen that the algorithm has high security performance.*

Keywords: *Cloud Computing, Block Chain, Logistics Transportation, Block Chain Model, Consensus Algorithm*

1. Introduction

As e-commerce enters the era of rapid development, the logistics industry has also developed rapidly. Internet + logistics quickly integrates e-commerce with logistics companies, and express delivery and express delivery have formed a huge modern logistics industry. A large number of logistics companies have contributed to the rapid development of my country’s economy and society. Played a huge supporting role. However, the current logistics industry service transaction system is highly centralized and has poor coordination capabilities. Blockchain is one of the hotspot technologies in recent years. Its essence is a huge decentralized distributed ledger database, which has the characteristics of decentralization, trustlessness, immutability and encryption. Apply blockchain technology to solve logistics data storage, logistics trust mechanism, logistics information encryption, realize decentralization, non-tampering, information traceability, transaction transparency, break industry barriers, promote fair competition, and bring positive effects to the logistics industry , Disruptive changes. Therefore, in the cloud computing environment, we apply blockchain technology to study the consensus algorithm of logistics service transactions, which has very important scientific significance and application value.

The logistics industry is loosely regulated. While maximizing benefits, it ignores the quality of logistics service transactions. The lack of trust in enterprise cooperation and the low cost of default have hindered the demands of high-quality enterprises to seek cooperation. Therefore, it is urgent to realize smart contracts to automatically reach a cooperative relationship and conduct cooperative transactions under the supervision of the entire network. For companies that are not standardized, they can quickly give feedback to get them out of the trading link.

DejeneBoru and his team see cloud computing as an emerging paradigm, providing computing resources as services over the network. Communication resources often become a bottleneck for the provision of many cloud application services. Therefore, copying data (such as a database) closer to the data consumer (such as a cloud application) is considered a promising solution. It allows to minimize network latency and bandwidth usage. They studied data replication in cloud computing data centers. Unlike other methods available in the literature, in addition to improving quality of service (QoS) due to reduced communication delays, they also consider the energy efficiency and bandwidth consumption of the system. The evaluation results obtained during extensive simulations help reveal the trade-off between performance and energy efficiency and guide the design of future data replication solutions [1]. David Yermack and his team believe that blockchain represents a novel application of the old problems of cryptography and information technology in financial record keeping, which may lead to profound changes in corporate governance. Many major players in the financial industry have begun investing in this new technology, and stock exchanges have proposed using blockchain as a new way to trade company shares and track their ownership. They evaluated the potential impact of these changes on managers, institutional investors, minority shareholders, auditors, and other parties involved in corporate governance. The lower cost, higher liquidity, more accurate record keeping, and transparency of ownership that the blockchain provides may greatly disrupt the balance of power between these groups [2]. Q.-S. Dou and his team found that the consensus problem in multi-agent systems has a wide range of application backgrounds in many fields such as sensor networks, social networks, and collaborative control. They researched the problem of discrete linear consistency algorithm with noise, and pointed out that the noise of discrete linear consistency algorithm is uncontrollable. To solve this problem, they proposed a strategy using noise suppression operator $\varepsilon(t)$. Control the noise, and point out that when the $\varepsilon(t)$ is high-order infinitely small at t-0.5, the noise of the consensus algorithm after noise suppression is controllable. They analyzed the influence of the suppression operator on the convergence of the consensus algorithm, and proved that under noise-free conditions, if the suppression operator $\varepsilon(t)$ is low-order infinitely small at t-1, the consensus algorithm after noise suppression can still converge to the original Convergence state x *. Based on this, they further pointed out that if the order of $\varepsilon(t)$ is between the order of t-0.5 and t-1, when $t \to \infty$, the state of all subjects will be a normal distribution with its center at the original position. Taking DHA as an example, the corresponding theoretical results are verified and discussed. They provide a theoretical basis for the noise control of linear consensus algorithms, and the determination of noise suppression operators has a strong directionality [3].

This article first studies and studies logistics service transactions, introduces the relevant application aspects of blockchain technology, analyzes different consensus mechanisms, and leads to consensus algorithms applicable to logistics blockchain. Aiming at the problem that the blockchain requires large-scale computing power in the context of the alliance chain, this article uses the practical Byzantine consensus algorithm as the basis to integrate the advantages of cloud computing, and gives the definition of logistics blockchain and cloud logistics blockchain. The calculated logistics blockchain model is based on the basic principles of the practical Byzantine consensus algorithm and the cloud logistics blockchain model, and combines the requirements of decentralization and non-repudiation to design a logistics blockchain consensus algorithm to build cloud-based logistics. Blockchain platform, experimental analysis of the performance of cloud computing-based logistics blockchain consensus algorithm.

2. ProposedMethod

2.1 Logistics Service Transactions

(1) Logistics service transaction model

Most logistics service transactions today use a centralized management model. The centralized logistics management platform integrates various logistics resources, so that logistics operation efficiency and costs are controlled. The logistics organizations work closely with each other to formulate detailed plans for the needs of each end-customer and collaborate to complete logistics services. The centralized management mode mobilizes the response capabilities of all parties in the platform, combines various software and hardware services to optimize the rapid response capabilities of logistics services, and analyzes the reasonable allocation and scheduling of resources through big data and logistics service systems to reduce logistics costs [4]. Cloud computing integrates open logistics service platforms, builds a centralized information sharing platform, and integrates e-commerce companies, logistics companies, and third-party payments. A centralized management platform for service transactions and the establishment of a real-time information monitoring mechanism to improve the quality of logistics services to a certain extent [5-6]. However, its transaction model relies heavily on centralized platforms, the information is not transparent, and the amount of data is excessively concentrated. A large number of small and medium-sized enterprises do not have the ability to build such a large-scale trading platform and cannot participate well in market competition [7].

(2) Logistics service transaction process

Today, most logistics service transactions adopt a centralized management model. The centralized logistics management platform integrates various logistics resources to control the efficiency and cost of logistics operations. The logistics organizations cooperate closely to formulate detailed plans for the needs of each end customer, and collaborate to complete logistics services. The centralized management model mobilizes the response capabilities of all parties on the platform, combines various software and hardware services to optimize the rapid response capabilities of logistics services, and analyzes the rational allocation and scheduling of resources through big data and logistics service systems to reduce logistics costs. The logistics service transaction process is shown in Figure 1:

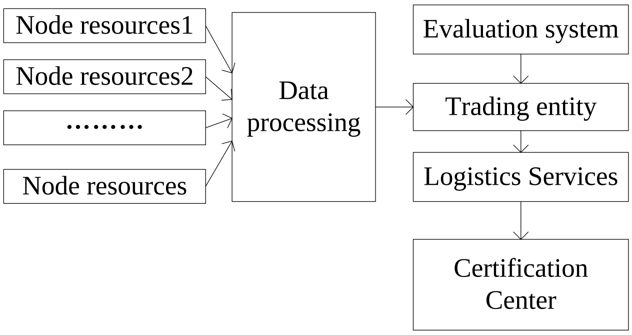

Figure 1: Logistics service transaction process

2.2 Block Chain Technology

(1) Blockchain technology architecture

Block chain is a database that is jointly maintained and de-trusted. It is a technology that combines encryption verification, game theory, consensus algorithm, and distributed storage [9]. It can be implemented in multiple programming languages and architectures. At present, common blockchain consensus algorithms include Proof of Work (POW), Proof of Stake (POS), and Delegate Proof of Stake (DPOS).

Combined with the definition of the blockchain, the blockchain needs to have four characteristics: Decentralized, Trustless, Collectively maintained, and Reliable Database [10].

(2) Decentralized network

The P2P network is a decentralized network structure. Nodes communicate with each other to realize resource sharing. The cloud computing network implements P2P network structure by creating virtual nodes in the cloud. Users connect to the cloud to implement resource monitoring and services. Its cloud computing server The interior is distributed. Through dynamic resource integration, the cost of user networking is reduced, and it has high reliability and high computing power [11-12]. Even if there are node failures in the entire network, high fault tolerance can avoid the wrong nodes. The shortest path selection algorithm is applied, and the node transmits data with less delay time and high efficiency.A data channel can be established directly between two nodes, or multiple adjacent nodes can be established connection, node resource sharing [13-14].

(3) Asymmetric encryption

The design of cryptography is used to ensure the security of all aspects of logistics service information circulation [15]. At present, the three types of non-pair encryption algorithms with the most influence are RSA, ElGamal, and Elliptic Curve Cryptography (ECC). The security of RSA depends on the difficulty of prime factorization of integers, and ElGamal and Elliptic Curve Cryptography (ECC) are based on solving discrete logarithm problems (DLP) and elliptic curve discrete logarithm problems

(ECDLP) over a finite field[16-17]. The elliptic curve cryptosystem has the advantages of short key length, fast signature speed, small calculation amount, fast calculation speed, good flexibility, and has higher security, lower overhead and delay [18]. Therefore, the current blockchain technology mainly uses the Elliptic Curve Signature Algorithm (ECDSA) to implement the information encryption design. Elliptic curves are derived from elliptic integrals:

$$\int \frac{d_x}{\sqrt{E(x)}} \tag{1}$$

Among them, $E(x)$ is a third-order polynomial and a fourth-order polynomial of x. An elliptic curve is described by the Weierstrassequation as:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2}$$

The determined curve, the set of infinite points 0 is the solution of the equation, where $a_i \in F, (i = 1,2,...,6)$, F can be the rational number field, the complex number field, or the finite field G (p) (prime p> 3) or $G(2^m)(m \in Z^+)$.

Elliptic curves are usually represented by E. If x = X / Z and y = Y / Z, substitute

$$(Y/Z)^2 + a_1(XY/Z^2) + a_3(Y/Z) = (X/Z)^3 + a_2(X/Z)^2 + a_4(X/Z)^2 + a_6 \tag{3}$$

When Z ≠ 0, it is sorted as follows:

$$Y^2Z + aXYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4X^2Z + a_6Z^3 \tag{4}$$

Define the following parameters:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \end{aligned} \tag{5}$$

Where Δ is the discriminant of the Weierstrass equation. When Δ ≠ 0 is satisfied, the elliptic curve is a non-singular curve, that is, the partial derivative that satisfies any point on the curve cannot be 0 at the same time. Then the above real number points can be used to construct the elliptic curve addition, and when Δ = 0, the points on the elliptic curve should not be constructed at this time.

The security of the Elliptic Curve Cryptography (ECC) used in the blockchain is also based on the Elliptic Curve Discrete Logarithm Problem (ECDLP). Bitcoin uses a special elliptic curve and a series of mathematical constants defined by the ecp256k1 standard.The secp256k1 curve is defined by the following function:

$$y^2 = (x^3 + 7) over(F_p) \tag{6}$$

$$y^2 \bmod p = (x^3 + 7) \bmod p \tag{7}$$

F_p shows that the curve is in the finite field of prime order p. Most Bitcoin programs use the OpenSSL cryptographic library for elliptic curve calculations.

(4) Digital signature

The logistics network transmits information, which does not exclude the interception and destruction of encrypted information by malicious nodes. In order to solve the problem of secure delivery and immutability of logistics service transaction information, each logistics node obtains and analyzes the logistics service transaction information of the previous node. After encryption, the digital signature of the node must be attached [19-20]. Each node transmits logistics service transaction information including a series of key pairs, and each key pair includes a private key and a public key. The private key (k) is usually a series of random numbers, and the necessary signature is generated to prove the correctness of the logistics service information. The elliptic curve encryption function is used to generate a public key (K), and the public key (K) is further subjected to a one-way encrypted hash function to form an encrypted digest (A) [21-22].

(5) Bitcoin's consensus algorithm

The most important in the blockchain are consensus algorithms, such as Proof of Work (POS), Proof of Stake (POS), and Delegated Proof of Stake (DPOS) [23]. It requires high computing power to obtain accounting rights or issue digital currency reward mechanisms. However, the logistics chain of trusted nodes requires an efficient consensus mechanism and does not need to issue virtual digital currency. Therefore, for a blockchain like the logistics chain, the distributed consensus algorithms PBFT (Byzantine Fault Tolerance), Paxos, and Raft are likely to be better choices.

Practical Byzantine Algorithm (PBFT) This is a consensus consensus algorithm based on message passing. PBFT has the advantages of short key length, fast signature speed, small calculation amount, fast calculation speed, and good flexibility. It has higher security, lower overhead and delay. Therefore, the current blockchain technology mainly uses PBFT to realize information encryption design. Its primary node (Primary) selection formula is:

$$p = v \bmod 3f + 1 \tag{8}$$

The message request format is

$$< REQUEST, o, t, c > \sigma_c \tag{9}$$

Its message request format is:

$$<< PRE - PREPARE, v, n, t > \sigma_p, m > \tag{10}$$

The message request format is:

$$< PREPARE, v, n, d, i > \sigma_i \tag{11}$$

Its message request format is:

$$< COMMIT, v, n, D(m), i > \sigma_i \tag{12}$$

2.3 Logistics Blockchain and Its Cloud Model

(1) Logistics blockchain cloud model

The blockchain technology is essentially a distributed demonstration technology. The so-called distribution type means that the data is not concentrated in a certain data server center, but is stored in each node in the network. The network members themselves are the data storage and carrier, directly sharing, storing and copying the data.

The realization of blockchain technology, combined with existing cryptographic techniques such as asymmetric encryption and hash arithmetic, has created a new consensus mechanism for solving the heterogeneous problems of distributed networks, and has created a new proof-storage technology. Among them, the asymmetric encryption technology is used to verify the identity of users, which is equivalent to providing a mechanism for customers to register "accounts" and "passwords". Hash operation is used to verify transactions and realize the consensus mechanism of workload verification, and is used to ensure the consistency of the information among the nodes in the blockchain network.

Blockchain technology itself does not innovate the underlying technology, but combines asymmetric encryption technology, P2P network, hash operation and other basic technologies to form a brand-new certification of decentralization technology. An important foundation of blockchain technology is cryptography. It can be said that without the related technology brought by cryptography, there will be no blockchain. This is why Bitcoin and other digital currencies are also called cryptographic currencies. The most important encryption technology used by blockchain technology is asymmetric encryption technology. The cloud computing-based logistics blockchain model is shown in Figure 2:

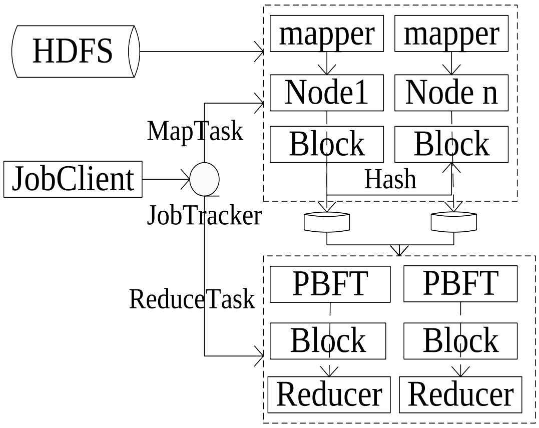

Figure 2: Logistics blockchain model based on cloud computing

As can be seen from Figure 2, based on the cloud computing logistics blockchain model, all transaction authentication behaviors are performed on the Hadoopblockchain cloud platform. Among them, the HDFS module is responsible for storing and updating the blockchain information, the Job Client module performs query operations and submits node task requests, the Map module assigns task nodes to transmit and update blockchain information, and the Reduce module completes the data processing through the consensus protocol; first, Map the function dynamically allocates n nodes to each transaction subject, simulating its transaction information transfer process, passing the logistics transaction information through the Hash encryption algorithm, and then applying the Byzantine Consensus (PBFT) algorithm to complete the authentication process, and then using the Reduce function for protocol processing,and the consensus process has high fault tolerance and security [24-25].

(2) Problem description of logistics blockchain

In the cloud computing-based logistics blockchain model, it is an abstract generalized problem model: In a decentralized network, when all nodes communicate reliably, malicious participating nodes or wrong nodes are allowed in the network. Blockchain consensus algorithm to ensure the integrity, traceability, and consistency of blockchain information, and store it in data storage nodes in a distributed manner.

At present, in addition to customizing the transportation plan through the relevant modules of the logistics information management system, and the simple management and tracking of the warehouse in and out of the warehouse, most of the operations still remain in manual management and paper document retention. The logistics transaction process includes order management, warehousing, inventory counting, transportation tracking, transaction feedback, etc. The detailed and sensitive information of the circulation links such as transportation costs, document review, transaction docking, and product integrity generated by this process is not uniformly processed. The entire logistics transaction process is invisible and cannot connect all customers in the supply chain to provide efficient The logistics services of China cannot meet the requirements of decentralization and non-repudiation of logistics.

The traditional logistics centralized transaction model has a certain degree of modernization, and an information platform is established through the operation specifications of the logistics center, the intelligent identification technology of the Internet of things, and the network and database of the logistics center. Users can conduct information inquiries and logistics transactions on their platform, so that once the centralized transaction information platform is attacked by hackers, the sensitive information in the database will be stolen, resulting in leakage of customer information; the user review mechanism is not perfect, leading to a flood of online registered users , It is impossible to prevent unfair competition such as false transactions; loss of goods and dishonest transactions in the logistics transportation process, etc., cannot trace the origin of the goods, and cannot collect comprehensive, complete and systematic logistics transaction information. The above-mentioned various problems cannot be properly solved under the traditional logistics centralization model. Therefore, it is proposed to apply cloud computing and blockchain technology to the logistics transaction model to achieve the purpose of decentralization, honest transactions, and traceability.

2.4 Blockchain Consensus Algorithm Based on Cloud Computing

(1) Basic idea of cloud logistics blockchain consensus algorithm

The PBFT algorithm is essentially a distributed consensus algorithm based on state machine replication. It is applied to the case where the number of fixed nodes is limited in the blockchain. Considering that the end users in the logistics network are not fixed, and there are situations in and out of the blockchain logistics network, it is necessary to solve the dynamic change perception problem of the classic PBFT algorithm. The consensus protocol consumes a lot of network bandwidth during the broadcast stage, requires a lot of node computing power to complete block verification and storage, and requires all terminals in the blockchain logistics network to deploy a large-scale cluster high-performance computing platform quantitative requirements. Aiming at the problem that the classic PBFT algorithm applied to the blockchain logistics network is not applicable, we propose a cloud computing-based logistics blockchain algorithm CloudPFBT, which will optimize the dynamic sensing of nodes, bandwidth consumption, stable communication, lightweight, and high throughput.

(2) Detailed algorithm design

1) Design of Map function

For Hadoop'sMapReduce execution mechanism, it is mainly divided into the mapper and reducer stages to process data. The JobTracker module reads the storage location information, and the Map module is assigned to assign TaskTracker to execute these block tasks.According to the custom Map function, the logistics information is encrypted and attached The digital signature is passed in the task node in a specific message format, and the input Hash data is divided into new key-value pair data tuples.The data tuple is the output of the Map function.The Map function is in the cloud computing-based logistics area. The blockchain consensus algorithm undertakes the block processing and communication of the logistics information blockchain, the hash encryption process, and the digital signature.

2) Design of Combine

In MapReduce, the Combiner receives the data tuple information output by the Map module as its input value, and uses the output <Key-Value> key-value pairs as the input to Reduce. The purpose of Combiner is to reduce redundant data, thereby reducing the load pressure on Reduce.

3. Experiments

3.1 Data Collection

In the express delivery network in the city, there are a total of n express companies that use the method in this article to conduct business. We use the PBFT algorithm to calculate these companies and test the security of the company's express delivery.

3.2 Experimental Environment

The experiments in this article were carried out on a notebook with Windows 10 system and 16G, 256G SSD memory. The cloud logistics blockchain platform is built using Hadoop.

3.3 Algorithm Flow

According to the cloud computing logistics blockchain model, a cloud computing-based logistics blockchain consensus algorithm is proposed. The algorithm steps are as follows:

Input: initial block data, key signature

Output: Cloud logistics blockchain information

Step1: A client sends a request in the request message and gives the initial value. This step is completed by the Input function.

The output of the number is a set of hash libraries, which are used as the input of the Map function;

Step2: The initial value receives the request, Jab Tracker assigns each node task, divides the parallel sub-bank, and assigns the task to 3f+1

Each mapper node node, node child node performs a hash function operation on the input, and attaches the node signature sign to generate a block-wide block broadcast. The network-wide node stores the block information;

Step3: The Mapper nodeNode performs a hash operation, and performs a first reduction on the Map result on each node through the Combiner function, and passes the reduced sub-base to the Reduce function;

Step4: The Reduce function combines the components passed by the Combiner and deletes the duplicate hash operation results.

The Reduce function is advanced through the three stages of pre-prepare, prepare, and commit of the PFBT algorithm.

Complete sub-library BInfoBlockchain Part combination to complete the service request;

Step5: The 2f+1 matching message is recovered, and the entire network authentication is completed, and the Jab Client feedbacks the information to the HDFS database for storage;

Step6: If the error node exceeds 51%, update the view and return the reinitialization request to Jab Tracker.

4. Discussion

4.1 Performance Analysis of the Algorithm

(1) Algorithm delay

Therefore, it can be measured according to the following delay indicators: delay time, broadcast time of logistics blockchain, execution time of consensus algorithm, confirmation time of logistics blockchain, and logistics node. The comparison and analysis results of the algorithm delay are shown in Table 1 and Figure 3:

Table 1: Algorithm delay comparison

	10	20	30	40	50
CloudPBFT	30	45	65	90	120
MinBFT	35	50	75	105	130
PBFT	40	60	105	145	175

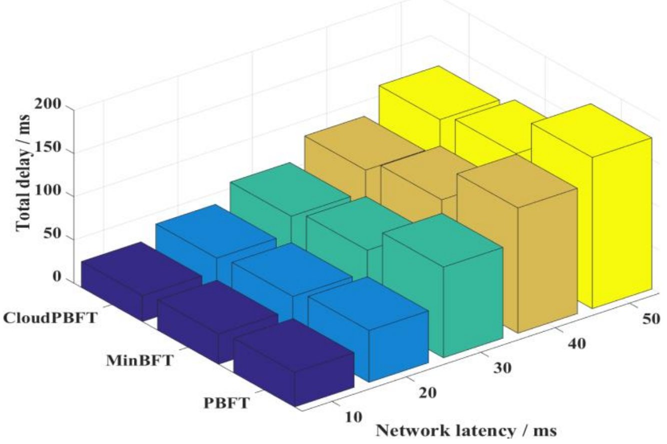

Figure 3: Delay analysis results of the algorithm

Under the same environment, by simulating the main node of the logistics transaction, the three algorithms all show an increasing trend in the network delay of 0-50ms, and the fluctuation is small, and the total delay of the unoptimized original PBFT algorithm is the largest. 0-30ms, the total delay of both the MinBFT algorithm and the CloudPBFT algorithm is basically the same, showing the level of network delay that the optimized consensus algorithm should have. Is the smallest delay, only 120ms. It is also found in experiments that the larger the node, the smaller the delay. It can be concluded that in the comparison of algorithm delays, PBFT>MinBFT>CloudPBFT shows that our algorithm has better advantages in network communication, and node fault tolerance fully utilizes the advantages of Hadoop cloud computing distributed node operations, which improves The speed of blockchain technology in the actual consensus authentication process.

(2) Throughput of the algorithm

Comparative analysis of the throughput of the algorithm is shown in Table 2 and Figure 4:

Table 2: Algorithm throughput comparison analysis

	10	20	30	40	50	60	70	80	90	100
CloudPBFT	26000	27000	30000	30000	31000	31000	33000	33000	34000	34000
MinBFT	18000	18000	18000	19000	20000	21000	22000	23000	24000	25000
PBFT	17000	18000	19000	20000	21000	20000	19000	18900	18800	18700

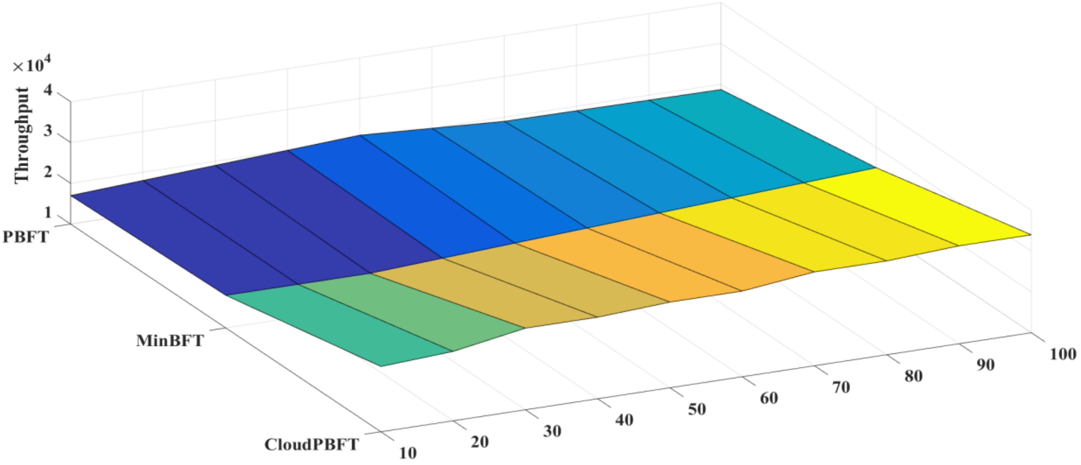

Figure 4: Comparison of throughput of the algorithm

It can be seen from Figure 4 that at 0-10 nodes, the throughput of the three algorithms shows a linear upward trend, and the throughput of CloudPBFT is the largest, reaching 26,000 times. The MinBFT algorithm shows a gentle trend at 20-50 nodes, and then continues to increase the number of nodes, the throughput increases with it, showing an upward trend, but it also tends to be saturated at 27,000 times. PBFT is between 10-110 nodes, the throughput performance is consistent, and there is a slight downward trend.

4.2 Algorithm's Fault Tolerance and Security Analysis

(1) Fault tolerance analysis of the algorithm

CloudPBFT algorithm can tolerate up to AA error nodes. Under the assumption of BB, observe the delay time and block height of the algorithm to determine the fault tolerance interval of the algorithm. The fault tolerance analysis of the algorithm is shown in Table 3 and Figure 5:

Table 3: Fault tolerance of the algorithm

	0	20	40	60	80	100
Algorithm delay	140	120	60	190	190	190
Block height	6000	4000	3000	900	900	900

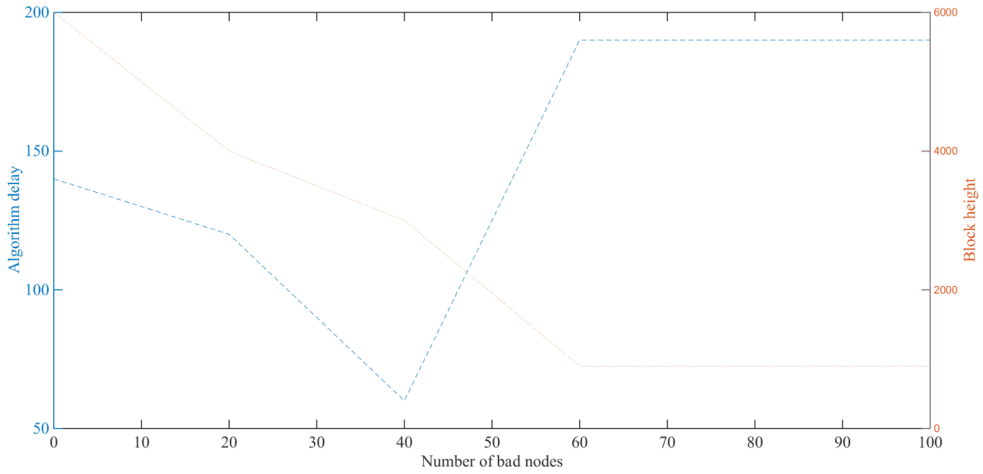

Figure 5: Fault tolerance analysis of the algorithm

As shown in Figure 5, the number of error nodes is between 0 and 40, and the algorithm's delay time shows a downward trend.

(2) Security analysis of the algorithm

We specify the probability that a certain number of fake nodes (ie, destroy nodes) control the entire network to indicate its security. The security analysis of the algorithm is shown in Table 4 and Figure 6:

Table 4: Security of the algorithm

	5	10	15	20	25	30	35	40	45	50
Attack success rate	0.3	0.2	0.05	0	0	0	0	0	0	0

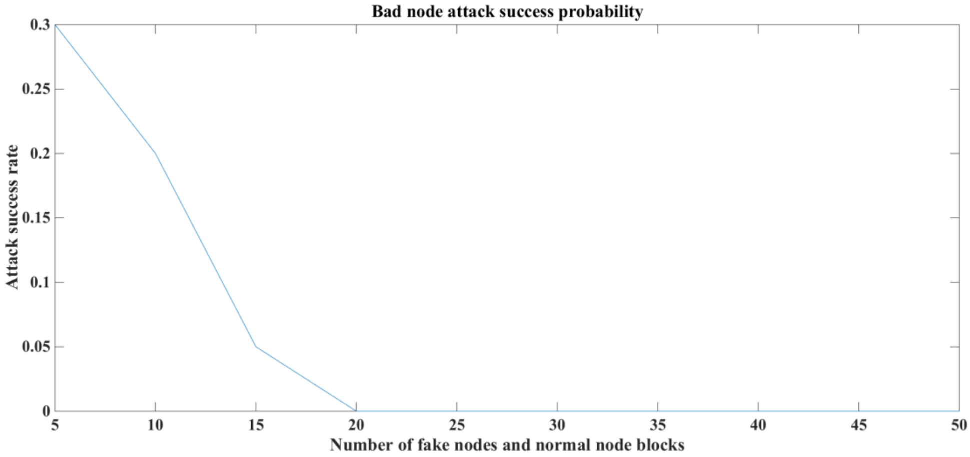

Figure 6: Security analysis of the algorithm

It can be seen from Figure 6 that the value of the fake block and the normal block increases, and the probability of successful attack shows an exponential decline.

5. Conclusions

(1) This article uses blockchain technology and cloud computing to design a cloud computing logistics blockchain model and a cloud computing-based logistics consensus blockchain PBFT algorithm to ensure decentralization and non-tamperable requirements. The high robustness of cloud computing and the characteristics of distributed storage are applied to solve the problem of computing power of large-scale consensus calculations. It provides a series of problems for the current logistics industry to deal with opaque transactions and other issues.

(2) This article designs a cloud computing-based logistics blockchain consensus algorithm.All operations are handled by the cloud. It is inevitable that the cloud will run out of control and cause the entire network to be paralyzed. The consensus process is divided into two tasks, Map and Reduce,

which can alleviate the burden on the blockchain system.

(3) The basic design idea of the algorithm proposed in this paper is to implement dynamic perception and improve the fault tolerance of the algorithm based on the practical Byzantine algorithm. By describing the main functions of the algorithm in detail, the algorithm flow is given, and the algorithm is compared with other optimization algorithms through experiments.

References

[1] DejeneBoru, DzmitryKliazovich, FabrizioGranelli. Energy-efficient data replication in cloud computing datacenters. Cluster Computing, 2015, 18(1):385-402.

[2] David Yermack. Corporate Governance and Blockchains. Social Science Electronic Publishing, 2017, 21(1):7-31.

[3] Q.-S. Dou, L. Cong, P. Jiang. Research on discrete linear consensus algorithm with noises. ActaAutomaticaSinica, 2015, 41(7):1328-1340.

[4] UdayVenkatadri, KasinadhuniShyama Krishna, M. Ali Ulku. On Physical Internet Logistics: Modeling the Impact of Consolidation on Transportation and Inventory Costs. IEEE Transactions on Automation Science & Engineering, 2016, 13(4):1-11.

[5] Melodena Stephens Balakrishnan. Aramex PJSC: carving a competitive advantage in the global logistics and express transportation service industry. Emerald Group Publishing, 2015, 5(3):1-54.

[6] Sparks W .Geospatial Analysis and Optimization of Fleet Logistics to Exploit Alternative Fuels and Advanced Transportation Technologies. Procedia Engineering, 2015, 121(5):309-316.

[7] Mario Guajardo, Teodor G. Crainic, Debjit Roy. Special issue on "Transportation and Logistics with Autonomous Technologies". International Transactions in Operational Research, 2020, 27(1):696-696.

[8] Caunhye, Aakil M, Zhang, Yidong, Li, Mingzhe. A location-routing model for prepositioning and distributing emergency supplies. Transportation Research Part E Logistics & Transportation Review, 2016, 90(43):161-176.

[9] Hanne Pollaris, Kris Braekers, AnCaris. Iterated local search for the capacitated vehicle routing problem with sequence-based pallet loading and axle weight constraints. Euro Journal on Transportation & Logistics, 2017, 69(3):304-316.

[10] Sarah Underwood. Blockchain beyond Bitcoin. Communications of the ACM, 2016, 59(11):15-17.

[11] WeizhiMeng, ElmarTischhauser, Qingju Wang. When Intrusion Detection Meets Blockchain Technology: A Review. IEEE Access, 2018, 6(1):10179-10188.

[12] Esther Mengelkamp. A blockchain-based smart grid: towards sustainable local energy markets. Computer Science - Research and Development, 2018, 33(1-2):207-214.

[13] SamareshBera, SudipMisra, Joel J.P.C. Rodrigues. Cloud Computing Applications for Smart Grid: A Survey. Parallel & Distributed Systems IEEE Transactions on, 2015, 26(5):1477-1494.

[14] Yumin Wang, Jiangbo Li, Harry Haoxiang Wang. Cluster and cloud computing framework for scientific metrology in flow control. Cluster Computing, 2019, 22(1):1-10.

[15] TarandeepKaur, InderveerChana. Energy Efficiency Techniques in Cloud Computing- A Survey and Taxonomy. Acm Computing Surveys, 2015, 48(2):1-46.

[16] Zijian Cao, Jin Lin, Can Wan. Optimal Cloud Computing Resource Allocation for Demand Side Management in Smart Grid. IEEE Transactions on Smart Grid, 2017, 8(4):1943-1955.

[17] JianShen, Member, IEEE. Anonymous and Traceable Group Data Sharing in Cloud Computing. IEEE Transactions on Information Forensics & Security, 2018, 13(4):912-925.

[18] Humphrey M. Sabi, Faith-Michael E. Uzoka, KehbumaLangmia. Conceptualizing a model for adoption of cloud computing in education. International Journal of Information Management, 2016, 36(2):183-191.

[19] LexuanMeng, Xin Zhao, Fen Tang. Distributed Voltage Unbalance Compensation in Islanded Microgrids by Using Dynamic-Consensus-Algorithm. IEEE Transactions on Power Electronics, 2015, 31(1):1-1.

[20] RanjanN ,BihariSoni B , Shraman B . An Efficient Technique for Image Mosaicing using Random Sample Consensus Algorithm. International Journal of Computer Applications, 2015, 118(16):22-26.

[21] Moreno Ambrosin, Paolo Braca, Mauro Conti. ODIN: O bfuscation-Based Privacy-Preserving Consensus Algorithm for D ecentralized I nformationFusion in Smart Device N etworks. ACM Transactions on Internet Technology, 2017, 18(1):1-22.

[22] Edmond Nurellari, Des McLernon, MounirGhogho. Distributed Two-Step Quantized Fusion Rules via Consensus Algorithm for Distributed Detection in Wireless Sensor Networks. IEEE Transactions on Signal & Information Processing Over Networks, 2016, 2(3):321-335.

[23] X. Zhang, T. Yu. Virtual generation tribe based collaborative consensus algorithm for dynamic generation dispatch of AGC in interconnected power grids. Zhongguo Dianji Gongcheng Xuebao/ proceedings of the Chinese Society of Electrical Engineering, 2015, 35(15):3750-3759.

[24] Yao Chen. Characterizing the Convergence of a Distributed Consensus Algorithm via Relative Hull. IEEE Transactions on Circuits & Systems II Express Briefs, 2015, 62(5):511-515.

[25] Jiahu Qin, Weiming Fu, HuijunGao. Distributed k-Means Algorithm and Fuzzy c-Means Algorithm for Sensor Networks Based on Multiagent Consensus Theory. IEEE Transactions on Cybernetics, 2016, 47(3):1-12.