MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

V.N. Karazin Kharkiv National University

School of Mathematics and Computer Science

Department of Theoretical and Applied Informatics

Master's Thesis

Comparative Analysis of Consensus Protocols in Distributed Networks

Author:

Final year Master's Program student,

specialty - Computer Sciences and Information Technologies,

educational program: "Informatics"

Liu Kaixuan

Supervisor: Kyrylo Rukkas

Reviewer: Kyryl Korobchynskyi

Adviser: Oleksandr Barskyi

Kharkiv, 2024

Comparative analysis of consensus protocols for distributed networks.

Head Record

Comparative analysis of consensus algorithms in distributed networks.

Conclusion: By carefully reviewing a large amount of information, we will clarify the background of the development and application of blockchain technology. Get an overview of the global research situation. Summary of research contents The research method and way of thinking can be summarized to clarify the importance of the research. And the goal is to explain the concept of decentralized networks and blockchain technology and the relationship between the two, focusing on analyzing the main consensus protocols of blockchain and their application fields, and introduce Pow, Paxos, Raft, and PBFT. Analysis of the advantages and disadvantages of various consensus protocol algorithms including DPoS, and the most important is security and transparency analysis. Through in-depth analysis and comparison, this paper finally concludes that the PoW algorithm has the best overall performance among the current public blockchain technologies. This is because the PoW algorithm has its own shortcomings. Therefore, this paper provides an improvement plan at the algorithm framework level. Compare the logistics improvements before and after through the flow chart. And theoretically analyze the intersection reduction according to the algorithm. Optimization improves the performance of the PoW algorithm and opens up a new way of thinking.

To others to study the algorithm related to the consensus protocol. It also helps to choose the consensus protocol in various situations.

Keywords: decentralization, network, consensus protocol. Distributed

1Related concepts

1.1 Representation of a distributed network

As a computer network architecture, distributed networks leverage their inherent distributed properties to distribute data, services, and applications across nodes in multiple physical locations. Building efficient, flexible, and robust networks There is no single control center for these networks. And each node can perform data processing and storage tasks. This greatly improves the reliability of the network. Even if some nodes fail, other nodes will continue to operate. This ensures that the entire network can continue to operate.

1.2 Blockchain Technology

Blockchain is a chain-like data structure consisting of blocks that are constantly increasing. They are linked using hash pointers. Blockchain data can only be added. It cannot be deleted or edited. It is a distributed network where each node has a local backup copy of the blockchain. The blockchain consensus protocol defines a set of rules that each node must follow. This ensures that the blockchain data of each node is ultimately secured in a decentralized system.

1.3 Relationship between distributed networks and blockchain

Blockchain specifically refers to a distributed ledger database technology with the characteristics of an immutable ledger and smart contracts. Distributed networks are a broader concept and do not refer to a specific technology. They include blockchains. However, they also include point-to-point file transfer systems. Distributed database systems, etc. [2] In general, blockchains are a form of distributed network technology applied. They utilize the distributed characteristics and consensus mechanisms of distributed networks. They have advantages in data processing. They enhance security and trust. Distributed networks are a broader concept that also includes blockchain technology.

1.4 Consensus Protocol Overview

Consensus protocols are a critical part of any decentralized network. And this is especially important in blockchain technology and decentralized applications. Because there is no central authority or trusted third party. This ensures that all participating nodes agree on the state of the network. This ensures the security, integrity, and consistency of the system. Nodes in a decentralized network do not directly trust each other and can consist of untrusted participants. The challenge of decentralized systems is to allow all nodes to reach consensus on the authenticity and accuracy of data without a trusted organization . This ensures that all nodes reach consensus on the transaction records. Create a blog about system state changes that maintain the stability and reliability of the Masu system.

The importance of consensus protocols is mainly reflected in the following aspects:

Ensuring data consistency: In a decentralized network, multiple nodes (or computers) are involved in storing and processing data simultaneously. Since there is no central controlling node, data consistency is a major challenge. A consensus protocol provides a unified set of rules and procedures that ensure that all nodes reach agreement on the "correctness" of a particular data state or transaction record[4].This maintains data consistency across nodes in the network. For example, in a blockchain, a consensus protocol ensures that: All nodes agree on the correctness of a blog. Thus, avoiding divisions and conflicts [5].

Ensuring network security: One of the main roles of consensus protocols is to prevent malicious attackers from manipulating data or performing attacks such as DoubleSpend on nodes through certain mechanisms (PoW, PoS sanctions, etc.). Irregular work is punished. This makes malicious actions expensive or difficult to implement. For example, Proof of Work (PoW) requires nodes to perform a large amount of computation. This makes it more expensive for an attacker to manipulate data. Therefore, only an attacker with more than 50% of the processing power can destroy the data. Network security [6] But requires a lot of resources

Decentralized trust mechanism: In traditional centralized systems,

trust is provided by a central authority (such as a bank, government, or cloud provider), whereas in a decentralized system, there is no single central authority [7], and the algorithms are designed and activated to replace the central authority. In a decentralized trust mechanism, the Bitcoin network uses Proof of Work (PoW) to reach consensus. This is where all nodes participate without intermediaries and reach consensus through competition and verification.

Solving the Byzantine General Problem: The Byzantine General Problem describes how a system can reach a unanimous decision among multiple participants who do not trust each other. Consensus protocols are designed to solve this problem. They help the system to function properly and maintain proper data consistency, even if some nodes are malicious or misbehaving. [7] Blockchain consensus mechanisms (PoW, PoS, etc.) solve the problem of malicious behavior of some nodes and network fragmentation by trusting the honest behavior of some nodes in the network.

Improved system scalability and performance: Consensus protocols not only ensure data consistency and security, but also optimize system scalability and transaction performance. Some powerful consensus mechanisms, such as Delegated Proof of Stake (DPoS) and Proof of Authority (PoA), enable faster block generation and higher transaction throughput. To meet the needs of decentralized networks with a large

number of users, some consensus protocols, such as Proof of Stake (PoS) in Ethereum 2.0 , are designed to improve system performance and scalability by reducing resource usage and increasing transaction confirmation speed.

Financial incentives and participation: Consensus protocols are not only used to ensure consistency and security. They also plan financial incentive mechanisms to encourage nodes to participate in network maintenance. For example, in PoW and PoS mechanisms, miners or validators earn block rewards or transaction fees by solving mathematical puzzles or staking cryptocurrencies [10]. They monitor system security and provide mining rewards to ensure the continued operation of the network. Thus, the security of the entire network is guaranteed [11].

Reduce the risk of a single point of failure: A centralized system relies on a single control node or server. This creates the risk of a single point of failure. If this node or server goes down, the entire system can be affected. A decentralized network relies on multiple nodes to jointly maintain the system. Avoid the risk of a single point of failure. Consensus protocols improve system fault tolerance by ensuring that all nodes participate in data verification and maintenance. This ensures that the entire network can function normally. Some nodes can fail or not function.

2 Analysis of traditional consensus algorithms

2.1 Portfolio Verification PoW is one of the most widely used

consensus algorithms today. First proposed in 2008, this algorithm uses cryptographic techniques to solve the problem of mistrust that can occur between nodes in a distributed network. And it is quite balanced in the process. In this situation, the problem of determining the decision-making authority for a proposal in an open system is solved. After continuous development and promotion, it has become the main consensus mechanism for cryptocurrencies around the world. The most famous applications are as follows : Within the Bitcoin network, PoW is a protocol that ensures the consistency and security of the blockchain network. In the PoW mechanism, nodes (miners) obtain a new block by “proving” the computational work of performing a complex mathematical problem . It is added to the blockchain and is rewarded accordingly. The basic steps [14] by a node executing the PoW algorithm are as follows:

1 Group all unconfirmed transactions into a transaction group. Include transactions that create coins. Send them to a new blog. Without exceeding the blocking limit.

This is the header of the header building block.

3 Enter different NONCE values and attempt successive hash operations until the block's hash value meets the difficulty requirement.

④ This node immediately broadcasts the discovered block to the network and mines the next block.

⑤ After receiving the block, other nodes immediately check the

legitimacy and difficulty of the block. And after confirming that the blog is legitimate and correct. Instead, stop mining locally and use the block to mine a new block to a new endpoint, distributing the block to the entire network.

Algorithm Advantages Because the difficulty adjustment mechanism of the PoW algorithm is large and the block size is fixed. Here, we will focus on the Bitcoin scenario. The block generation speed can be estimated at 600 seconds per block, the minimum size of each transaction is 250 bytes, and the throughput is about 7 transactions per second [14].

Applications: Currently, all consensus algorithms used in existing blockchain applications are PoW (Bitcoin, Ethereum, Litecoin, etc.) and are the most common consensus algorithm today.

Cost Control: There is no limit to the number of nodes. Therefore, if the number of nodes is sufficiently large, the risk of manual control is very low and the cost of control is very high.

Power consumption: With unlimited nodes and continuous high-speed hashing, the Bitcoin network can perform hundreds of billions of SHA256 calculations per second [15].

Consensus Speed: To reduce the risk of network fragmentation, the PoW algorithm uses a difficulty control algorithm to ensure a stable block generation rate for this network.

Shared : The network is open to all nodes for access and termination.

Upper limit on number of nodes: There is no upper limit. The more nodes you have, the higher the control cost and the better the system security.

Purpose: Nodes operate independently and cannot detect when other nodes in the network are generating new blocks. Therefore, the structure of the hash operation is unpredictable. And since a node broadcasts a block through the network as soon as it generates it, multiple nodes can simultaneously send the newly discovered block to the network. And theoretically, if the processing power is sufficiently powerful, malicious nodes can also appear on the network at the same time. We will compute the block from scratch. However, this problem can be solved. To solve the problem, add manual checkpoints. This defeats the original purpose of the PoW algorithm [17].

Key features of PoW:

Security: 51% attack: Compromises the security of the blockchain. The attacker must control more than 50% of the processing power. If the attacker has more than 50% of the processing power, they can create fake blocks and falsify transaction history. This leads to problems such as double spending attacks. Although this attack is difficult and expensive, it still poses a threat to PoW networks.

1 Decentralization: In PoW, all nodes can participate in mining. Therefore, theoretically, there is no risk of centralization. Mining work is

usually concentrated in a few large mining pools. This depends on the concentration of processing power.

2 Computing Resources and Power Consumption: Power Consumption: The main disadvantage of PoW is the high computing demand and high power consumption. Miners must invest a lot of computing resources to successfully mine a new block. As a result, energy loss. The energy consumption of the Bitcoin network has been criticized, especially in relation to the global energy crisis and climate change.

Incentive Mechanism: PoW encourages miners to contribute to network maintenance and security through a reward mechanism for "mining" (Bitcoin or other cryptocurrencies) and mining fees for solving puzzles, verifying transactions, and creating new blocks[18]. This mechanism ensures consensus on network security in a decentralized network without relying on a central authority.

④ Abuse prevention: The throughput requirements of PoW make it difficult to modify blocks once they have been generated. Even if an attacker can change a block, they will have to recalculate the hash of each block after that block. This requires a huge amount of processing power.

2.2Evidence of effort

In 2011, people interested in digital currencies proposed the Proof of Stake (PoS) algorithm in Quantum Mechanics[19].The PoS algorithm uses a similar taxation competition mechanism to the PoW algorithm, and

considers account balances and currency depreciation as competition factors. The biggest advantage of this algorithm is that it uses very little energy. Since it can reach consensus without relying on hash operations, all nodes in the network of the PoW algorithm will keep trying. They will perform hash operations until they find a common value that satisfies the difficulty requirement. Then, they will set the difficulty requirement high enough to find a new block. It has been proven that the block is very difficult to solve the ledger authentication problem [20]. However, the difference between the PoS and PoW algorithms is that PoS does not require hash operations. However, it does consider whether a node has accounting rights. It is determined by multiplying the node's account balance and the account period. This balance is maintained. The account with the highest product value gets the account rights for the block at that height. After obtaining the accounting rights, the holding period is reset to 0. And the product value also returns to 0. Therefore, nodes can only be accumulated. Once the value of the product becomes sufficiently large, it can return to competition for accounting rights [21].

Efficiency: The PoS transaction feature is highly scalable, because each node knows in advance which node will be forging the next block, and transactions can be sent directly to the Forge node.

Cost Control: There is no limit to the number of nodes. Therefore, if there are enough nodes, the risk of manual control is very low. However,

the cost of control is very high.

Power Consumption: There is no limit to the number of nodes, but the PoS algorithm consumes less power than PoW because nodes do not need to perform hashing operations. To participate in the mint, you only need to keep the node online, which respects the algorithm.

Consensus speed: Blockchains using the PoS algorithm can maintain a faster block speed. This is because it is expected that accountants will not create multiple blogs at the same time. This allows for higher throughput than the PoW algorithm.

Openness: The network is open to all nodes to access and output without access restrictions.

Upper limit on number of nodes: There is no upper limit. However, the more nodes you have, the higher the control cost and the better the system security.

Purpose: As with the PoW algorithm, nodes operate independently and cannot detect whether other nodes in the network have created a new block. Therefore, when a node creates a block, that block is immediately broadcast through the network [Twenty-Two], which has no purpose of its own.

2.3Byzantine fault tolerance in practice

The PBFT algorithm was proposed by Miguel Castro and Barbara Liskov in 1999 to solve the general Byzantine problem. Compared with the

BFT algorithm, this algorithm has improved performance. It greatly reduces the algorithm complexity. And it can realize applications with Byzantine fault tolerance. It also provides fault tolerance even if less than 1/3 of the nodes fail or fail [23]. The PBFT scheme can be considered as a copy algorithm. Here, the state machine is copied between all nodes. All copies of the state machine maintain the service state. The PBFT algorithm tries to ensure that all nodes maintain the same replica state. And all nodes take corresponding actions to achieve this goal [24]. Clustering requires three basic protocols: Consistency protocol. Checkpoint protocol and Interface switching protocol. In this article, we will focus on the first protocol. The privacy procedure mainly includes the steps of preparation, request, response, preparation, and confirmation.

Algorithm process:

Step 1 Preparation

(1) The master node receives a request from the client. It sets up a code request and sends initial information to the remaining slave nodes. (2) When the master node receives the pre-provisioning information, node 1 receives the pre-provisioning information. After generating the code, proceed to the next step.

② Preparation stage

(1) Node 1 receives an encryption request from the master node and sends a ready message to the master node and the remaining slave nodes. If

not sent, your proposal will not be accepted. (2) When Node 1 receives a clear message about the consent number sent by other slave nodes, it indicates that Node 1's status is ready, and at this time Node 1 receives the prepared certificate.

3 Steps to Verify Serial Number

(1) After node 1 enters the ready state. The node immediately sends authentication information to the remaining nodes (2). When node 1 receives more than 2/3 of the authentication information, node 1 completes the authentication transition (3). It is considered to have transitioned to standby mode. And each node that requested has accepted the number assigned by the parent node. The cluster node moving to the verified state means that the customer's request has been fulfilled.

HyperledgerFabric's performance aspect performance measurement results adopt the industry consensus PBFT algorithm. The performance was found to exceed 10,000 operations per second.

In terms of usage, Hyperledger Fabric, a popular open source blockchain project by IBM, currently uses the PBFT consensus algorithm. [24] Domestic applications include digital currencies developed by central banks. Ant Financial's blockchain applications and Ant Digital Currency, Coin, etc.

Cost control: Mainly used in centralized organizations or cooperative enterprises. The number of nodes is limited. There is a risk of human

manipulation due to the public consensus algorithm of the blockchain. Low control cost.

Power consumption: Since the number of nodes is limited, energy consumption levels can be controlled.

Consensus speed: The number of nodes is limited, and consensus can be reached quickly through messages.

Opening: Opening is difficult and too many nodes will corrupt the network.

Maximum number of nodes: Limited

Purpose: Once a record is processed, it cannot be edited. Therefore, it has its original purpose. Once the transaction is confirmed, there are no changes. Additionally, the transaction is considered completed.

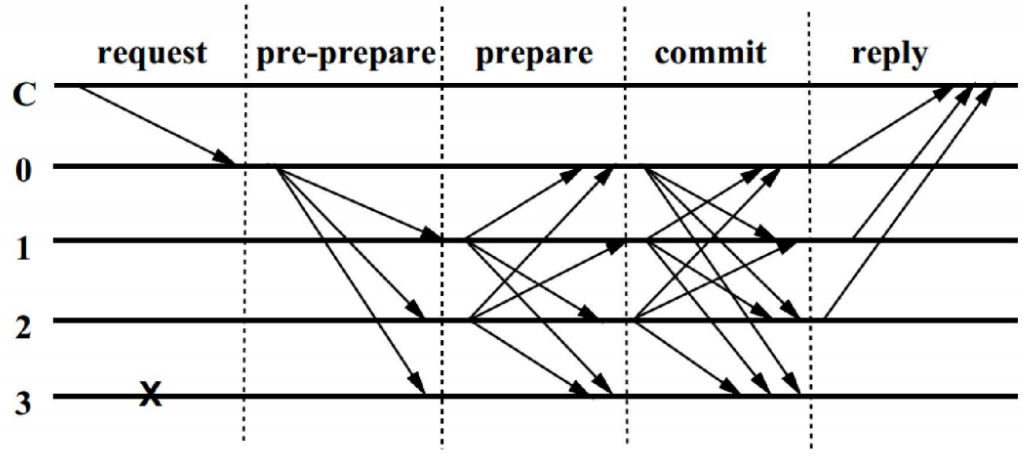


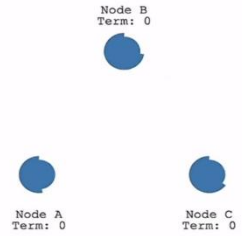
Figure 1. Schematic illustration of the PBFT algorithm.

2.4Raft

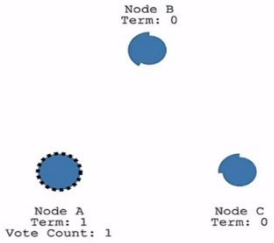
The Raft algorithm was published in 2013 by Diego Ongaro and John Ousterhout of Stanford University in a paper titled

"InSearchofanUnderstandableConsensusAlgorithm". This algorithm is based on the Paxos algorithm and has a fault-tolerant capability that can handle half the failure of nodes [25] compared to the Paxos algorithm. Engineering practice. The process of reaching consensus through the Raft algorithm is as follows. All nodes subscribe to the leader's recommendation. The manager has accounting authority at this point. The client submits a change. The leader completes the accounting and generates a block, and the leader transmits the block to other nodes. The specific process of this algorithm is as follows. During the election process, each node in the cluster has its own polling timer. And this time it is randomly generated. So when C's timer expires, there is essentially no self-introduction at the same time. As soon as the node expires, the other nodes send an automatic recommendation signal. Since the timer has not expired yet, the other nodes see that node C is the unconditional leader node and broadcast this message to the other nodes in the cluster. However, the notification data from node C comes back early. Therefore, the timer is reset before it runs out. The selection process starts again until node C becomes unavailable [26]. The algorithm flow is as follows.

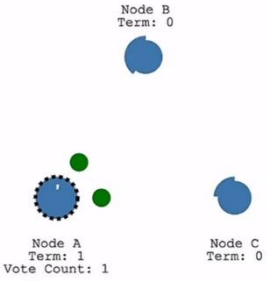
1


Node B
Term: 0
Node A
Term: 0
Node C
Term: 0

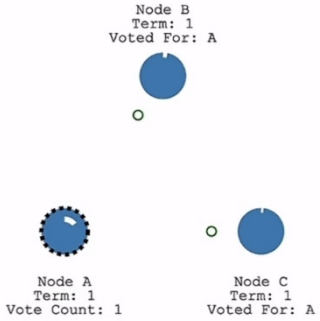
2


Node B
Term: 0
Node A
Term: 1
Vote Count: 1
Node C
Term: 0

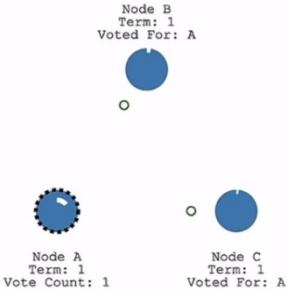
3


Node B
Term: 0
Node A
Term: 1
Vote Count: 1
Node C
Term: 0

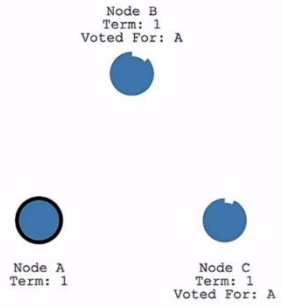
4


Node B
Term: 1
Voted For: A
Node A
Term: 1
Vote Count: 1
Node C
Term: 1
Voted For: A

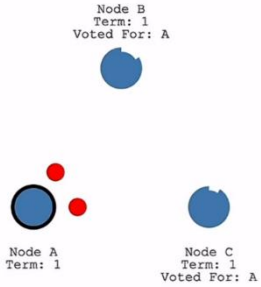
5


Node B
Term: 1
Voted For: A
Node A
Term: 1
Vote Count: 1
Node C
Term: 1
Voted For: A

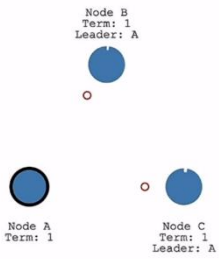
6


Node B
Term: 1
Voted For: A
Node A
Term: 1
Node C
Term: 1
Voted For: A

7


Node B
Term: 1
Voted For: A
Node A
Term: 1
Node C
Term: 1
Voted For: A

8


Node B
Term: 1
Leader: A
Node A
Term: 1
Node C
Term: 1
Leader: A

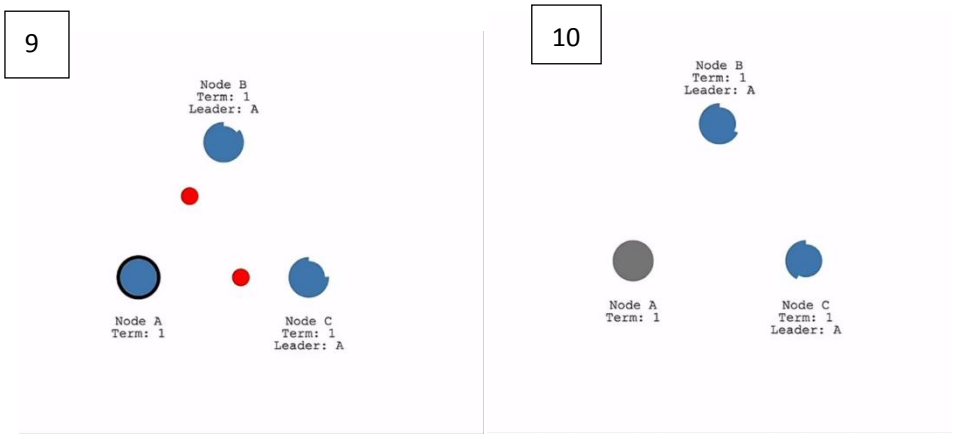


Figure 2Algorithm Flowchart

The specific process of log replication is as follows: The leader node receives an update request from a client. Sends the update request information to other nodes in the cluster. The leader node verifies the update request data. The leader node copies the update request locally and sends the completed update data to the client. The leader node performs the update on other nodes in the cluster. Complete the main compliance contract for the update request process. The algorithm flow is shown in the image below.

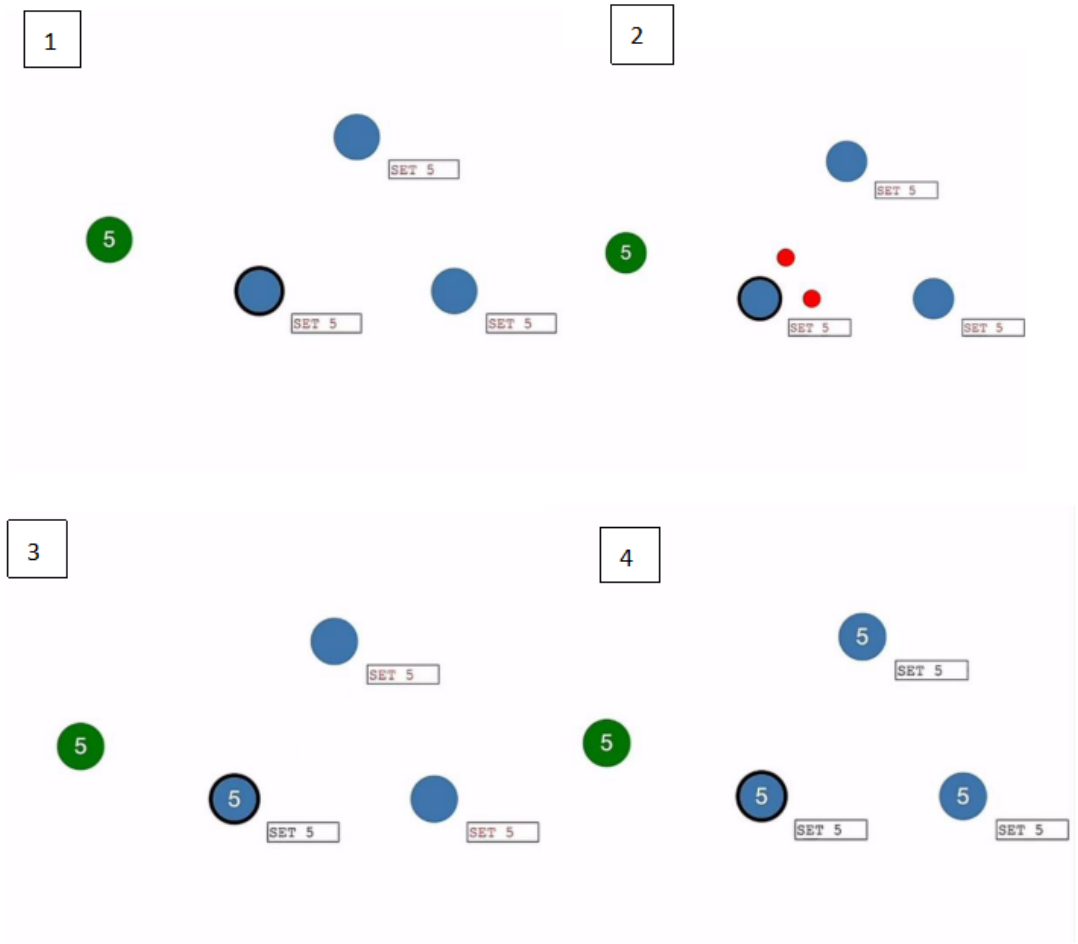


Figure 3. Log replication flow diagram.

Performance Raft's original algorithm test performance can reach 10,000 to 30,000 transactions per second.

Current projects using fleet algorithms on the side include Etcd, Kubernetes, and Baidu Cloud Storage.

Cost management: Mainly used in centralized organizations. The number of nodes is limited. There is a risk of false regulation due to the public consensus algorithm of blockchain. Low management costs.

Power Consumption: Since the number of nodes is limited, power consumption levels can be controlled.

Consensus speed: Due to the limited number of nodes, consensus can be reached quickly through messages.

Sharing : It's hard to start, and too many nodes can break the network.

Regarding the upper limit of the number of nodes: There is a limit.

Purpose: Once a record is processed, it cannot be edited. So it had its original purpose. So once a transaction is confirmed. It cannot be changed and the transaction is considered closed.

2.5 Paxos Algorithm This algorithm was introduced by Microsoft researcher Leslie Lamport in 1990 and was intended to solve the general Byzantine problem that he had proposed eight years earlier. It is the first fault-tolerant algorithm for distributed systems that was proposed and put into practice. The general Byzantine problem discusses the principle of nodes. How can data exchange be used to reach consensus in a distributed cluster? If the information that is relied on to reach consensus is destroyed, decisions are made on inconsistent proposals [27] . This breaks the consistency of the system. The Paxos algorithm was designed to solve this problem. And even in an asynchronous communication environment and when only a majority of nodes are available, the Paxos algorithm can lead the cluster to reach consensus[28].The roles of a system using the Paxos algorithm are as follows: proposer, decision maker, problem raiser, and learner who makes the final decision[29]. The execution process of the Paxos algorithm is as follows.

1) Preparation

(1) The proposer selects the nth proposal and sends a request for preparation to all decision makers. The decision makers submit proposals with the highest number of RFPs that are sent back to the sponsor, with the promise that RFPs with numbers lower than n will not be accepted.

2) Select

(1) If the proposer has received initial responses from multiple decision makers, the request for approval should be sent to these decision makers. (2) If the decision maker receives a proposal to accept application number n, it accepts the proposal immediately, without breaking any commitments to other applicants [30] .

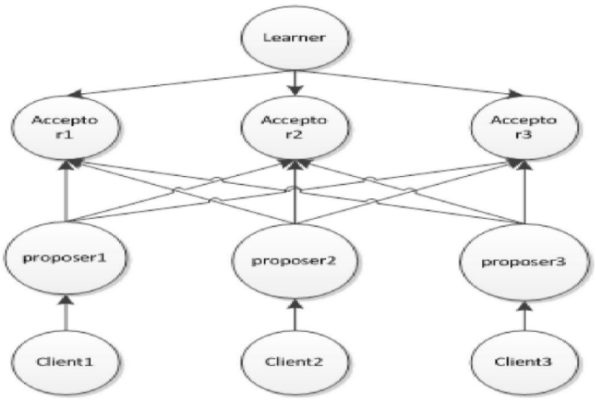


FIG. 4 Flowchart of PAXOS algorithm

In terms of efficiency, the test throughput of the algorithm built into Paxo can reach 10,000-30,000 transactions per second, which can basically meet the workload requirements of current commercial payment application scenarios.

In terms of cost management, it is mainly used in centralized

organizations and the number of nodes is limited. Therefore, there is a risk of human manipulation due to the public consensus algorithm of the blockchain. Low management cost

Power Consumption : The number of nodes is limited, so you can control the level of energy consumption.

As for the consensus speed, it is because the number of nodes is limited, so consensus can be reached quickly through messages.

From an openness perspective, it is difficult to open a network. And if there are too many nodes, the network will collapse.

There is a limit to the number of nodes.

As for the purpose, recordings have their original purpose because once processed, they can no longer be edited.

2.6 Algorithm Comparison Analysis

2.6.1 P2P architecture algorithm and non-p2p architecture algorithm can be classified into p2p network architecture consensus algorithm and non-p2p network architecture consensus algorithm. Based on the difference in network configuration format, the search algorithm included in this article includes the P2P network architecture consensus algorithm, including the PoW algorithm, the PoS algorithm, and the consensus algorithm for non-P2P network architecture. Paxo's PBFT algorithm and Raft algorithm are included due to their different consensus processes. As the network size changes, each algorithm in the consensus network model

has different communication volumes corresponding to different network sizes , so the network continues to grow. Therefore, the communication volume generated during the consensus process increases dramatically. And all nodes must communicate with each other. When communication occurs, nodes continue to initiate consensus tasks. Network congestion increases and throughput continues to decrease. This eventually leads to network paralysis. Paxos and Raft algorithms are not designed to be Byzantine fault tolerant. They can only provide services when less than half of the network nodes are present (downtime network interruption), so achieving consensus on a public blockchain is not ideal. In addition, since these algorithms achieve consensus through messages, the criteria for node status also need to be improved. This is because it must be guaranteed that nodes know information from other nodes. Everything in the network Nodes meet the network requirements, but they lack the network visibility required for public networks. [33]Unlike p2p architecture algorithms, non-p2p architecture algorithms achieve consensus properties through message passing. This can prevent intersection problems and improve consensus performance. However, in these types of algorithms, each node must send a message to reach consensus. Therefore, the communication formula is $T=O(n^2)$, where n is a suitable wedding ring for Number or a wedding ring that is only applicable to private channels. As the number of nodes increases, the communication volume also increases significantly.

When used in a public network, significant delay and congestion occur in the network [34], so this type of consensus algorithm is not suitable for application situations with a large number of nodes, such as public blockchain applications. The main target at present is data storage with a small number of basic nodes, such as databases and logs.

2.6.2 PoS and PoW Algorithms The PoS algorithm has several important advantages over the PoW algorithm.

1) The PoS algorithm uses account balances and currency age as competitive indicators and can reach consensus without performing hash operations. This results in very low energy consumption [35].

2) Blockchains using the PoS algorithm can maintain a faster block speed. This is because the auditors can know in advance that multiple blocks will not be generated simultaneously, which allows for higher throughput than the PoW algorithm.

The PoS algorithm also has the following drawbacks:

1) Because accounting authority is predetermined, there is a risk of malicious nodes attacking double spending.

2) Fairness Collapse Attack In the PoS algorithm, nodes try to explore through different branches. This effort is not costly on an ongoing basis, since it does not require hashing operations. This makes the main chain vulnerable to the problem of many branch chains. This does not affect the overall security of the network. Nodes are either honest or malicious. They

will try to obtain as much information as possible. Based on the principle of profit maximization.

This is due to the consensus algorithm used in the public network. The algorithm must meet the following basic requirements: Transparency. There is no barrier to entry into the network system. Nodes can enter and exit the network freely. High control costs are a small cost. Complete control over the entire network is quite high. The control network meets the investment financial conditions. The return after regulation should be very high. Consensus algorithms for non-p2p network architectures such as Paxos, Raft, PBFT, and DPoS algorithms have advantages in terms of transmission efficiency and energy consumption. This is difficult to match with consensus algorithms for non-p2p network architectures, but it matches. The above mentioned two basic conditions. From a security perspective, these algorithms cannot be used as public chain consensus algorithms . However, the PoS algorithm is more open than the PoW algorithm and has a much lower energy consumption level. Therefore, the network is vulnerable to attacks. Therefore, the tendency to generate blocks is obvious from a security perspective, so the PoS algorithm cannot guarantee the security of transactions.

2.7 Overview of this chapter

This first chapter provides a detailed analysis of the principles and architecture of current traditional consensus algorithms. We analyze these

algorithms in terms of control costs, energy consumption, unanimous speed, openness, and the maximum number of nodes. We analyze and compare various network architectures, algorithms, PoS algorithms, and PoW algorithms in detail to find out the advantages, disadvantages, and applicable scenarios of different resolutions. And we can conclude that the PoW algorithm is the most suitable consensus algorithm for the following purposes: Public blockchains today.

3. Forking problem of PoW algorithm.

3.1 Cause of the problem Blockchain technology is a distributed ledger technology. Here, all nodes in the network cluster participate in obtaining accounting authority and maintaining the ledger. Mutual verification of dataData has changed from being stored in a central organization to being distributed and stored in individual nodes [37]. In order to gain trust in a distributed knowledge center, data consistency between nodes must first be guaranteed. In other words, consensus must be reached between nodes. Various illegal operations of nodes that meet the consensus requirements are performed simultaneously. All legitimate data nodes throughout the network work together to resist maintaining network consensus. In this way, consistent results can be obtained, which are the same as those of central enterprise data storage. At the same time, it is time to maintain a fully automated network system. The intervention of a central authority and the risk of falsifying personal data for various

organizations are no longer necessary · Therefore, achieving network consensus and maintaining data consistency are the most important prerequisites for decentralizing a blockchain network. However, as a blockchain network, it is the largest chain in the world. Currently, there are nearly 10,000 full Bitcoin nodes, and ensuring and maintaining consistency across such a large number of nodes is a major challenge for consensus algorithms. [39]The portfolio determines the size of each block as 1 MB, while the mining difficulty mechanism ensures a constant rate of generating new blocks approximately every 10 minutes. This parameter directly leads to very high throughput. According to Bitcoin's transaction data structure, the minimum data size of a transaction is 250 bytes. Therefore, the throughput of the Bitcoin network can be calculated as approximately 7 transactions per second [40]. This is the main reason why Bitcoin cannot be an electronic payment method. The reason Bitcoin is structured this way is mainly due to the following considerations: The p2p network environment conditions at the time of Bitcoin's launch: If the block is too large, it may result in overly large blocks. Network delay. In a multi-hop p2p network, blocks are spread out, and new blocks are generated too quickly. This causes some nodes to generate invalid blocks in the fourth step if the transaction bandwidth is not saturated. Reducing the block size requires a full node to store all the blockchain data. Disk space is scarce and full. This reduces the cost of running a node. This

indirectly encourages people to participate in the distribution of computer nodes. Increasing the number of Bitcoin processing nodes increases the processing power of the entire network. This makes it more expensive for malicious nodes to perform double-spend and data manipulation attacks. This increases data security transactions. Although the block size is only 1 MB and the block interval is 10 minutes, the more nodes there are in the entire network, the longer it takes to discover a block and propagate it throughout the network. Blocks are completely distributed across the entire network. Previously, a new block of this height was discovered by a set of nodes that did not contain the data for the new block. Just because a fork occurs does not mean that the transaction is complete. And multiple block confirmations are required before a transaction is considered complete and secure. The Bitcoin system lacks timeliness, which is a major obstacle to the development of this technology.

3.2 Architecture Analysis

Due to the problem of the PoW algorithm, Bitcoin users cannot immediately confirm whether the transfer is successful. And if there is a concern about forgery during the transfer, it takes a long time to confirm the forgery. Please wait a moment. Although this process can ensure the security of the transaction [43], in the PoW algorithm, it takes a long time for the node to receive the second block. Today, nodes that maintain the same height as the best chain do not reject it completely. However, the branch

with the node falls to the backup chain that is slower than the backup chain. The branch is detected and extended to enable block reordering. This requires multiple verifications to ensure the security of the transaction. It is important and prerequisite for financial operations to ensure the safety of the operation by making a certain concession when confirming the transaction. [44] From a probabilistic point of view, block forks occur intermittently. However, as the number of nodes in the network increases, the total processing power of the network increases. The difficulty of the network also increases. We found that as the number of hash operations required for a block increases, the block generation speed is constant and the probability of splitting decreases.

3.3 Nature of the problem

Currently, Bitcoin users generally believe that after six confirmations of a transaction on the Bitcoin network, the probability of a transaction being completed or altered is close to zero. This view raises two questions: Why do transactions need to be confirmed by the network? And why do transactions need to be confirmed six times for the first question[45]First, we need to understand the process of reaching consensus in the PoW algorithm. Bitcoin's distributed consensus consists of four independent verification processes on each computer node.

1) All nodes verify all transactions according to the consensus mechanism.

2) All nodes verify the newly received block and join the most appropriate chain branch.

3) When a new blog is verified, all transactions in the local transaction group are packaged.

4) Since Bitcoin is a decentralized P2P architecture system, each node independently selects the best chain branch based on the longest chain principle and the load accumulation principle. Therefore, there is no centralized maintenance system in traditional centralized institutions. Therefore, availability and reliability are high. When sending a remittance request through the Internet, the sender's transaction request is not strictly guaranteed. There is no guarantee that the data will be transmitted to the node on the network, but there is no guarantee after the transaction is received. The node completes the transaction in a local transaction block and compresses it into a local block. Wait until the next block is generated before displaying the block. Check if the transaction you sent is included in the transaction. If there is network congestion, you can check if your transaction has been confirmed by the network and recorded in the block · If there are too many transactions to be confirmed or the transaction fee is too low, your transaction will not be given priority. You may have to wait a long time for the network to confirm the script.

Therefore, the nature of blockchain transactions that require network verification is that the blockchain system does not have a central authority

to verify transactions. The transaction is considered confirmed. Second question. Even though a transaction is confirmed by the majority of nodes in the network, this does not mean that it is secure. Each node in the network operates independently and cannot detect whether other nodes in the network have created a new block. Therefore, when a node discovers a new block, it immediately broadcasts it to the network. This is because the result of the hash operation is unpredictable. A fork occurs when several nodes distribute newly discovered blocks to the network over a period of time and two new blocks appear on the network at the same time. The longest chain principle of the PoW algorithm allows two attackers to compete for the accounting rights in the next block in the network. When a new block is created, this means that this branch is longer than the other branches. This border block is recognized by the entire network. The opposite branch is deleted. And the transaction history of the abandoned block is no longer visible. Therefore, there is a risk of verifying a block that has been transmitted only once. Although unlikely, additional confirmations are required to ensure that the transaction has been successfully completed to enhance security. It is generally believed that this happens when a transaction is confirmed 6 times. The risk of forgery is virtually zero. It is important to compare the processing power of these nodes. Therefore, even if only a small number of nodes confirm the transaction, the transaction is confirmed and verified by as many nodes as

possible throughout the network through multiple confirmations. The processing power of the entire network is very low. And the probability that a new block will be found on these nodes is also very low. Therefore, the risk of the transaction being tampered with is virtually zero. From the analysis above, the problem of confirming a transaction multiple times ensures that as much network processing power as possible is used to secure the transaction. Minimize the possibility of the transaction being altered as much as possible. [47] It can be seen that this is the target of .

3.4 Overview of this chapter

In this chapter, we first study the problem of long transaction confirmation in blockchain applications using the PoW algorithm, and then explain the main causes of the problem through probability theory. We sort out the hidden probability problems. We perform probabilistic simulations using programming. We continue to identify the root causes of the problem.

4. PoW Algorithm Improvement Plan

4.1 Improvement Measures

The PoW algorithm calculates the difficulty of a block in the following height range. It calculates the average time for a given number of blocks before the current block. It achieves the goal of maintaining block interval stability. Computation and editing requirements This is due to the uncertainty of the hash operation. This timing mechanism can guarantee

the total distance between blocks of a certain length. within a given range, but it cannot guarantee that the range of each block is close to the average. Therefore, if many nodes discover and publish a new block in a short period of time, the network will be split.

The current PoW algorithm works as follows: when the same node receives several new block transmissions of the same height during a block cycle. In the first step, the cumulative throughput of the two shared blocks is determined after the block verification. The cumulative throughput of the block is equal to the throughput of the local block. Therefore, if the blog is a legitimate blog. Then, the block is placed on the backup chain, and the node remains on the block it initially received. According to the principle of the longest chain, one of the fork branches runs until the fork height is extended for the first time, at which point the blockchain network leaves the fork state and reaches a consensus. [48] And a deeper investigation into the logic shows that the original PoW algorithm reduces the fork probability and the number of block confirmations required to ensure safe transactions. By allowing the consensus process to occur. The first block of the intersection is completed in advance and finalized by consensus. This reduces the risk of crossings. This means that the risk of transactions being manipulated is reduced. It also reduces the number of confirmations required for transactions.

The design concept is as shown in the figure below.

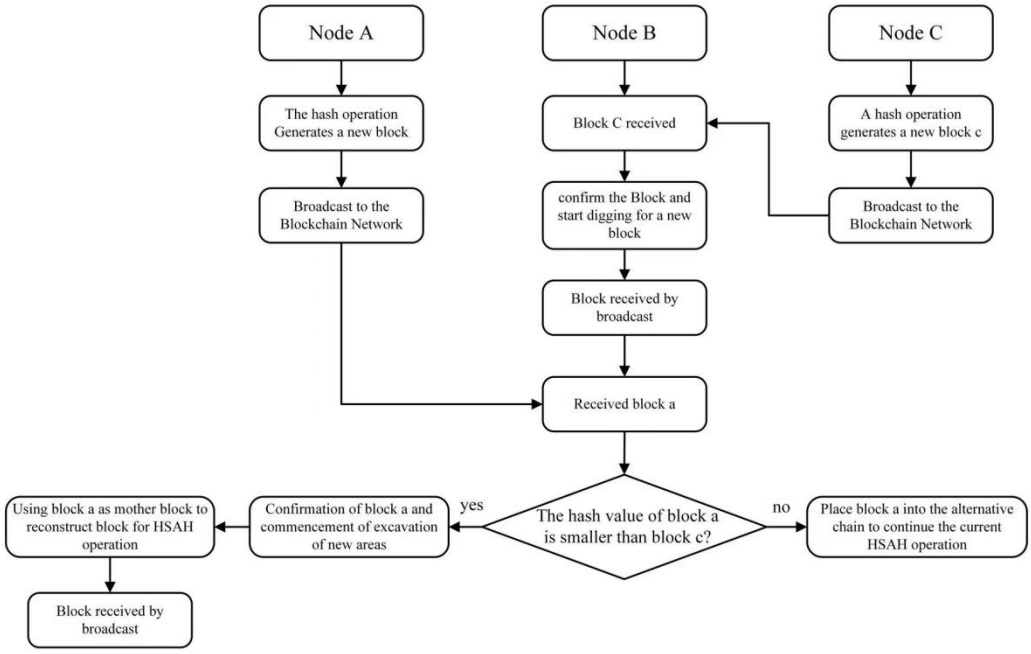


Figure 5PoW algorithm fork algorithm processing flowchart has been improved.

If we improve the existing PoW algorithm, it is the same as the above process. The node can go through the deposit process. After receiving the blog, the node must decide whether to mine the block at this height without wasting the completed work. Invest in mining blocks at the next height. If we continue to dig this blog. This process can continue indefinitely. And if the node in the network chooses to continue mining the block, the length of the block can no longer increase according to the maximum profit principle [49]. If the block is successfully broken, other nodes will do the same. We will face the situation of rejecting the mined block. Similarly, compared to the processing power of the entire network, the probability of a block being found by the computing power of one

node is lower than the probability of a block being found by another node. In order for the entire network to maximize its profit, the node chooses to maintain the current height, and the mined block is immediately moved to the next level of mining blocks.

The logic of the optimized algorithm is as follows: When the same node receives several new transmissions for blocks of the same height during a block cycle. In the first step, the cumulative throughput of the two separated blocks is determined. Then, it is checked whether the block is an If block. The block is a valid block. The node immediately compares the hash values of all blocks at that height. And the node determines the block with the highest difficulty value as the direction in which to extend the main chain. Does mining continue after this node? We analyze the decision-making process of the node between the two points in the blockchain system. If the hash value of the block received from the node is less than, it indicates that the challenge was successful and the node stops at the current value immediately. Mining block. Add the original block to the backup chain. Replace the most suitable end of the chain with the block obtained later. Dig that block. At the same time, the blog is broadcast as a webcast. If the hash difficulty of the block received from the node is relatively high, it indicates that the challenge failed. And the node adds it to the backup chain and continues the current mining operation. If the network only has these two branches, then when a blog

is published on the next branch, the network fork state will end. Before accessing the entire network, a new block will be created on another branch according to the principle of the longest chain. And this new block will accumulate more work. Therefore, the entire network accepts the point where the block of the alternative chain is placed as the optimal chain. At the same time, nodes must reconstruct the block to get out of the fragmented state of the network.

4.2 **Algorithm Improvement**

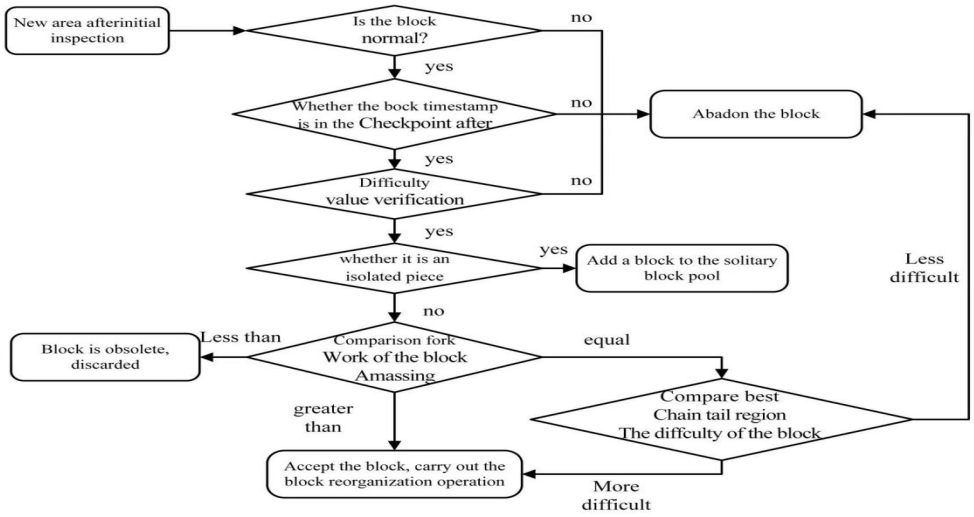


Figure 6PoW algorithm fork algorithm processing flowchart has been improved.

The specific processing steps for intersections when obtaining a block with the same height as the optimal end block through an improved algorithm are as follows: (The best end block is called a defense block, and the block obtained later becomes the highest block. (The end block of the chain has the same height as the defense block. The block with the same

height as the Jia end block) The chain is called a challenge block. It gets a defense block and a challenge area accordingly. The value of the accumulated workload for the block. If the accumulated number of defense blocks and challenge blocks is the same, the data, the hash values of the two blocks are compared. If the hash value is larger, an error is returned, otherwise, when the workload is accumulated, it starts to reconstruct the optimal blockchain. The challenge block is larger than the defense block. This means that the challenge branch is extended. Here's how to generate two sub-blocks of the chain in a short time. At this time, the challenge branch is longer than the optimal branch flow of the node, and when the challenge block workload is accumulated, it has an optimal blockchain structure with more accumulated workload. If it is smaller than the guard block, the challenge will fail, and theoretically, no blocking will occur during the extraction process.

4.3 Overview of this chapter This chapter first explains the plan for improving the PoW algorithm of this paper from an architectural perspective. That is, the goal is to optimize the fork and consensus process to reduce the probability of forks and eliminate the probability of long forks, which is explained in the flowchart. The logical difference before and after the algorithm improvement and its impact on the branching state before and after the algorithm improvement are theoretically analyzed.

5 Summary and Trends

5.1 Overview of the work

Consensus algorithm is the foundation of blockchain technology. It is considered a basic condition for strengthening the reliability properties of blockchain. In this article, we examine the current consensus algorithm in detail. We develop a vision for optimizing existing algorithms. We improve the efficiency of the proof-of-work mechanism and promote the practical application of high-quality blockchain technology.

The main content of the report is the introduction of blockchain technology from its origin and the development of blockchain technology and consensus algorithms. Understand the current status of domestic and international research, and analyze the current status of blockchain technology and consensus algorithms at domestic and international levels. After explaining the current status of research in this field, explain the research purpose and significance of the paper in detail to clarify the original intention of the paper and the value of the research content included in the application. Agree on the Proof of Work algorithm, and finally introduce the main research content, research ideas, and methods of the paper. For example, summarize the content of the article, present the problem of long transaction confirmation time in the app, explain the PoW algorithm, and then define the problem and summarize the important issues. The above analysis explained the concept of optimizing

the PoW algorithm. This paper describes the improvement plan of the PoW algorithm at the architecture level. And the logical differences before and after the algorithm improvement are shown in the flowchart. Analyze the theoretical branching situation before and after the algorithm improvement.

5.2 Future Outlook

Blockchain technology plays a key role in transforming data transmission networks into valuable networks. And it is a forward-looking and imaginative technology that can greatly reduce the cost of transmitting valuable data to Internet users. This paper has completed an optimization study on the fork problem using the workload-tolerant consensus algorithm. However, if an improved algorithm is used, the possibility of fork can be greatly reduced. However, from a security perspective, the completeness of the architecture and the algorithm optimized for the actual operation of the application can affect the stability of the block interval, for example, and the time compensation of the block interval mechanism can be optimized in a targeted manner. At present, the research potential of blockchain technology is enormous. And there are high expectations for the efficiency and security improvements that blockchain technology will bring to the fields of finance, technology, commerce, and personal consumption. New technologies and developments are discovered.

6 References

[1] BonneauJ, MillerA, ClarkJ, NarayananA, KrollJA, FeltenEW.Sok: Perspectives and research questions on Bitcoin and cryptocurrencies. IEEE Security and Privacy Symp.

[2]NakamotoS.Bitcoin:APeer-to-PeerElectronicCashSystem.WhitePaper. 2008.

[3]BeigelO.Merchants accepts BitcoinPayment.2019.

[4] IBM Financial Services 2019

[5]Blockchain Anti-Finance 2019

[6] IBM Supply Chain 2019

[7] Blockchain Government Association. 2019.

[8]Ethereum dapp market. 2019.

[9] Cryptocurrency Market Cap in 2019

[10] Bitcoin Verification 2019.

[11] EyalI, GencerAE, SirerEG, VanRenesseR.Bitcoin-NG: A scalable blockchain protocol. In: Proc.ofthe13th USENIXSymp.onNetworkedSystemsDesignandImplementation.2016.

[12] Sompolinsky, Zohara Secure and fast transaction processing in Bitcoin, in: Proc.de laConf.Int'l.on Financial Cryptography and Data Security.

[13] GarayJ, KiayiasA, LeonardosN.TheBitcoinbackboneprotocol:Analyticandapplications.In:Pro

c.oftheAnnualInt'lConf.ontheoryandApplicationsofCryptographicTechniq ues.20 15.281−310 [14] Gilad Y, Hemo S4, Mcho R, M. Algorand: Updated Zantian consensus sizes for cryptocurrencies: Proc.

[15] KogiasEK, JovanovicP, GaillyN, KoffiI, GasserL, FordB Improving Bitcoin security and performance with pooled signatures: Proc.

(16) MillerA, XiaY, CromanK, ShiE, SongD.

(17) Buterin V. Ethereum White Paper

[18]Coblee.Litecoin: The final version of Bitcoin, released in 2019.

[19] Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, DeCaro A, Enyeart D, Ferris C, Laventman G, Manevich Y. Hyperledger Fabric: A Decentralized Operating System for Permissioned Blockchains In: Proc. Part EuroSysConf.

[20] Gramoli V. From Blockchain Consensus to Byzantine Agreement: The Computer System of the Future

[21] Nguyen GT, Kim K. A Survey on Consensus Algorithms Used in Blockchain. Journal of Data Processing Systems

(22) WangW, HoangDT, HuP, XiongZ, NiyatoD, WangP, WenY, KimDI, A survey on consensus mechanism and mining strategy management in blockchain networks, IEEE Access.

[23] YuanY, WangFY Blockchain: State of Mind and Future Trends. ActaAutomaticaSinica, 2016, 42(4):481−494. (Summary in Chinese and English)

[24] Kiayias A, Russell A, David B, Oliynykov R. Ouroboros: A proven-secure proof-of-stake protocol In: Proc. of the Annual International Conference on Cryptology.

[25] LiC, LiP, ZhouD, YangZ, WuM, YangG, XuW, LongF, YaoACC Decentralized blockchain with high throughput and fast verification (Proc.delaconf.techniqueannualeUSENIX).

(26) Lewenberg Y, Sompolinsky Y, Zohar A. Comprehensive Blockchain Protocols I: Proc.

(27) CastroM, Liskov B.Practical Byzantine Fault Tolerance.In:Proc.oftheUSENIXSymp.onOperatingSystemsDesignandImplementation

(28) Mazieres D. Stellar consensus protocol: A federated model for internet-scale consensus I: Proc.

[29] Burrows M. Fat lock services for loosely coupled distributed systems, in: Proc.

(30) LamportL.Paxosmadesimple.ACMSigact News

(31) Lamport L, Shostak R, Pease M. General Byzantine problems. ACMTrans.onProgrammingLanguagesandSystems, 1982, 4(3):382−401.

(32) PeaseM, Shostak R, Lamport L. Reaching consensus despite obstacles: Air Force Commander Review

[33]RABINMO.Probabilisticgorithms[M].In:TraubJF,ed.AlgorithmsandComplexity.NewYork:AcademicPress,

[34]RABINMO.RandomizedByzantineGenerals[C]//24th Annual Symposium on Foundations of Computer Science; Tucson, AZ: IEEEpress.

Another advantage of the BONE SNAKE free option. (Additional Summary): Fully asynchronous compliance.

Protocol [C] // Proceedings of the ACM Symposium on Principles of Distributed Computing, New York: Air Chief Marshal.

Press 1983: 27-30.

(36) Dolevdi's strong polynomial algorithm for Byzantine agreement. [C] // Proceedings of the 14th ACM conference.

Symposium on Computer Theory, New York: ACMPress.

[37] FISCHER, M., LYNCH, N. Lower time limits ensuring consistency of interaction,data.

Processing Letter [J]

[38]TOUEGS.Randomized Byzantine Agreement[C]//3rd ACMS Symposium in progress

Vancouver Computer Distribution Principles British Columbia, Canada: ACMPpress;

(39) Shamirah, How to Share Secrets [J]

(40) Brachak, Toeks Asynchronous Consensus and Broadcast Protocol [J]

[41]BRACHAG.AnAsynchronous(n-1)/3-ResilientConsensusProtocol[C] //Proceedings Third ACM

Symposium on Distributed Computing Principles, Vancouver, British Columbia, Canada: ACMPpress;

(42) Kachinz, Kurzavec, Chupivi Randomized Prophecy of Constantinople: Practical Asynchronous Byzantine Covenant with Cryptography[J] Journal of Cryptography, 2005, 18(3): 219-246.

(43) CACHINC, KURSAWEK, PETZOLDF, etal.SecureandEfficientAsynchronous BroadcastProtocols[C]//AnnualInternationalCryptologyConference.Berlin, Heidelberg: SpringerPress;

[44] CHANDRATD, TOUEGS. Unreliable fault detector for reliable distributed systems[J]. Journal Flyshefsmarskalk,

(45) Mustafah Mostefouia Reynalm Synkron bysantinsk konsensus utan underskrifter och

t <*n* /3andO(*n* 2)Text[C]//Proceedings of the ACM2014 Symposium on Principles of Distributed Computing, New York: Air Force General.

[46]BRACHAG. Asynchronous Byzantine Agreement Protocol[J]. Data and Computation.

[47]SRIKANTHT.K,TOUEGS.Certified broadcast simulation for achieving simple fault-tolerant algorithms[J] Distributed computing.

(48) Ben-Orm, Kelmerb, Rabint, Asynchronous Secure Computing with Optimal Flexibility. [C]//Proceedings of the 13th Annual ACM Symposium on Principles of Distributed Computing.
New York: ACMP Press.
[49]MILLERA, XIAY, CROMENK, et al.ThehoneybadgerofBFT protocol[C]//implemented in 2016
ACMSIGSAC Conference on Computer and Communications Security,
New York: ACMPress.