# Current Status and Trends of Blockchain Consensus Mechanisms

Yujie Yang*

School of Cybersecurity, Northwestern Polytechnical University, Xi'an, Shaanxi, China

* Corresponding author: Yujie Yang (060614@mail.nwpu.edu.cn)

## Abstract

**Since the introduction of Bitcoin in 2008, the blockchain technology as its underlying architecture, has attracted attention from various sides due to its decentralized and distributed computing characteristics. AS the core advantage of blockchain technology, the consensus mechanism determines various characteristics of blockchain, such as security, scalability, and decentralization. Currently, there are many consensus mechanisms suitable for different scenarios. This paper studies the existing consensus mechanisms from the perspectives of algorithm principles, performance, etc. Firstly, this article divides the existing consensus mechanisms into Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT). Secondly, for each type of consensus mechanisms, the study analyzes their algorithmic principles, understands typical solutions and latest ones, clarifies the advantages, disadvantages, and the possible attack methods of various consensus mechanisms. Finally, the paper defines the basic requirements for new consensus mechanisms. It aims to help break through the application bottlenecks of blockchain technology and promote the development of blockchain technology in various scenarios.**

## Keywords

**Blockchain, consensus mechanisms, distributed systems, consistency.**

## 1. Introduction

In the current era, when the digital wave sweeps across the globe, with the increasing spread and application of digital currencies such as Bitcoin, blockchain, with its decentralized distributed ledger characteristics, has attracted great attention from government departments, financial institutions, and the technology industry, and has become a key force in reshaping the trust system and business models. In 2008, Satoshi Nakamoto[1] published <<Bitcoin: A Peer-to-Peer Electronic Cash System>>. This paper first mentions the concept of blockchain, pointing out that blockchain, as the underlying technology for constructing Bitcoin's data structure and encrypting the transmission of transaction information, supports the mining and transaction processes of Bitcoin and has become the cornerstone of the digital currency ecosystem.

Blockchain is essentially a decentralized distributed ledger database, which integrates technical elements such as peer-to-peer networks (P2P), asymmetric encryption, consensus algorithms, and reward mechanisms. Relying on these technologies, blockchain has established a new model that does not require endorsement from a centralized authority, allowing nodes to directly conduct trusted transactions and carry out collaborative cooperation. It provides an innovative idea for solving problems such as high costs, low efficiency, and data security risks in the traditional centralized model.

The consensus mechanism is the core of blockchain technology. In a P2P network environment where nodes lack trust, the process by which the preset consensus mechanism guides these untrusted nodes to achieve data consistency is called consensus. As a core component of blockchain, its key value lies in solving issues such as security, efficiency, and scalability. It

enables all honest nodes to maintain a consistent blockchain view, achieve data consistency, and synchronize the ledger information of each node.

Currently, mainstream mechanisms such as PoW, PoS, and PBFT have shown unique advantages in different application scenarios. However, they also expose problems such as the high energy consumption of PoW, the possible "stake concentration" caused by PoS, and the limited applicable scenarios of PBFT. With the continuous expansion of blockchain application scenarios, from financial payments to supply chain traceability, and from government affairs on-chain to IoT data collaboration, stricter requirements have been put forward for the efficiency, security, and scalability of consensus mechanisms. In view of this, it is significant to conduct in-depth research on blockchain consensus mechanisms, analyze their principles, evolution paths, and application limitations, and then explore new types of consensus mechanisms more suitable for future development needs.

This study focuses on blockchain consensus mechanisms, centers on the key point of typical consensus mechanisms, compares and analyzes the advantages and disadvantages of various mechanisms from the perspective of algorithm principles, and identifies the shortcomings of typical mechanisms. At the same time, combined with the diversified needs of the industry, it explores the design direction of new-type mechanisms to promote the development of blockchain technology.

## 2. Typical Consensus Mechanisms and Their Variants

### 2.1. PoW Consensus Mechanisms and Its Variants

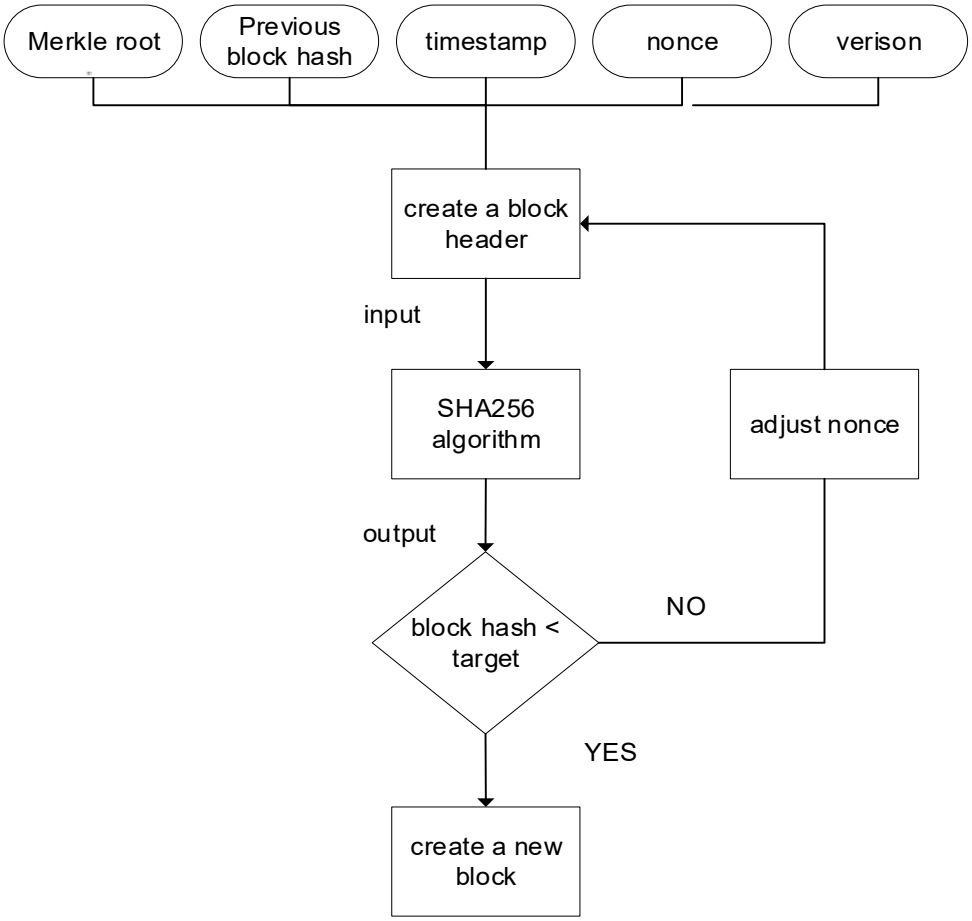


**Figure 1.** PoW Schematic Diagram [2]

PoW was first proposed by Dwork and Naor[2] in 1992, initially used to solve the spam problem, and later introduced into the blockchain field by Bitcoin as the core consensus mechanism. As shown in Figure 1, its basic principle is "computational power competition". Nodes first integrate their own addresses, timestamps, hash values of the previous block, and other information to generate block headers. Then, with the block header as the input, the block hash value is calculated through the SHA256 algorithm. Next, the hash value is compared with the node's coin age. If the coin age is greater than this value, the node creates a new block; if not, the node waits to participate in the next round of competition. In addition, to ensure the stability of block generation time (such as 10 minutes per block for Bitcoin), the difficulty will be dynamically adjusted according to the overall network computing power. The PoW consensus mechanism based on computational power competition not only has a high degree of decentralization, allowing any node to participate without identity verification, but also effectively ensures the security of system data. Attackers need to control more than 51% of the overall network computing power to tamper with data, which is extremely costly. However, the PoW consensus mechanism also has obvious shortcomings. Firstly, the competition for computational power requires a large amount of computing power input, resulting in low energy utilization. Secondly, the block generation time is slow and the throughput is limited, which is far behind mainstream financial transaction systems. Ordinary users find it difficult to participate in bookkeeping due to insufficient computing power, and the trend of mining pool monopoly is gradually forming.

In 2013, the Ghost protocol was proposed by Sompolinsky and Zohar [3]. Based on the principle of the heaviest subtree, when a fork occurs in the blockchain, the Ghost protocol calculates the number of blocks in each sub-block tree as the "weight" of the fork, and takes the fork with the maximum weight as the main chain, as shown in Figure 2.

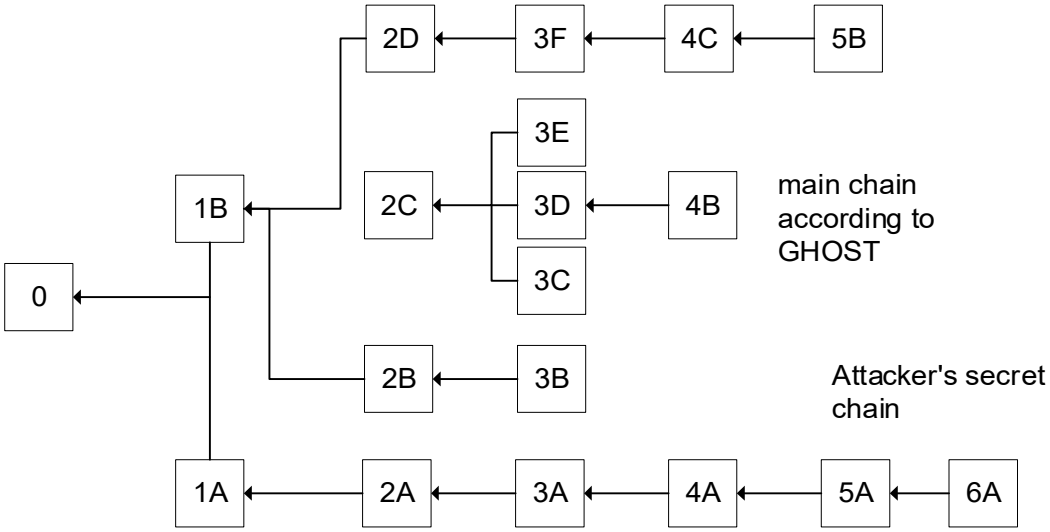


**Figure 2.** Schematic Diagram of Ghost Selecting the Longest Chain [3]

In 2016, Eyal et al. proposed Bitcoin-NG [4]. Bitcoin-NG conducts two basic operations: "leader" selection and transaction serialization within each 10-minute epoch, and generates key blocks and micro-blocks. Compared with traditional PoW consensus mechanisms, Bitcoin-NG can reduce system latency and increase throughput rate, has good scalability, but is difficult to solve the spending problem.

To address the huge energy consumption of PoW, in 2024, Tan Minsheng, Xu et al. [5] proposed an improved PoW-based consensus mechanism called Improved Proof of Work(IPoW). On the basis of PoW, IPoW reduces the absolute dominance of computing power over obtaining

accounting rights, and adds new factors such as node online duration and transaction history credibility to comprehensively evaluate a node's accounting qualifications, so as to avoid a purely computational power competition.

## 2.2. PoS Consensus Mechanism and Its Variants

The PoS consensus mechanism was first proposed by Quantum Mechanic [6] in 2011. The rule of PoS for determining the right to keep accounts at the next moment is almost the same as that of PoW. In PoW, the probability of miners successfully finding hash values is roughly positively correlated with their computing power; while in PoS, the success probability is proportional to the size of the stake (the product of the amount of digital currency and the holding time).

Delegated Proof of Stake(DPoS) was proposed by Daniel Larimer [7] in 2014. As shown in Figure 3, nodes holding stakes vote for candidate nodes. If a candidate node receives more than 50% of the votes, it becomes a delegated node. After that, the delegated node D[i] is allowed to create blocks in sequence (through $i++$ iteration). If D[i] successfully generates a new block, other delegated nodes will verify it; if not, D[i] is deleted, and the next delegated node is selected through re-iteration for an attempt. This ensures the orderly creation of blocks and the achievement of network consensus, and simplifies the block generation process by voting to elect delegated nodes, thereby improving efficiency.

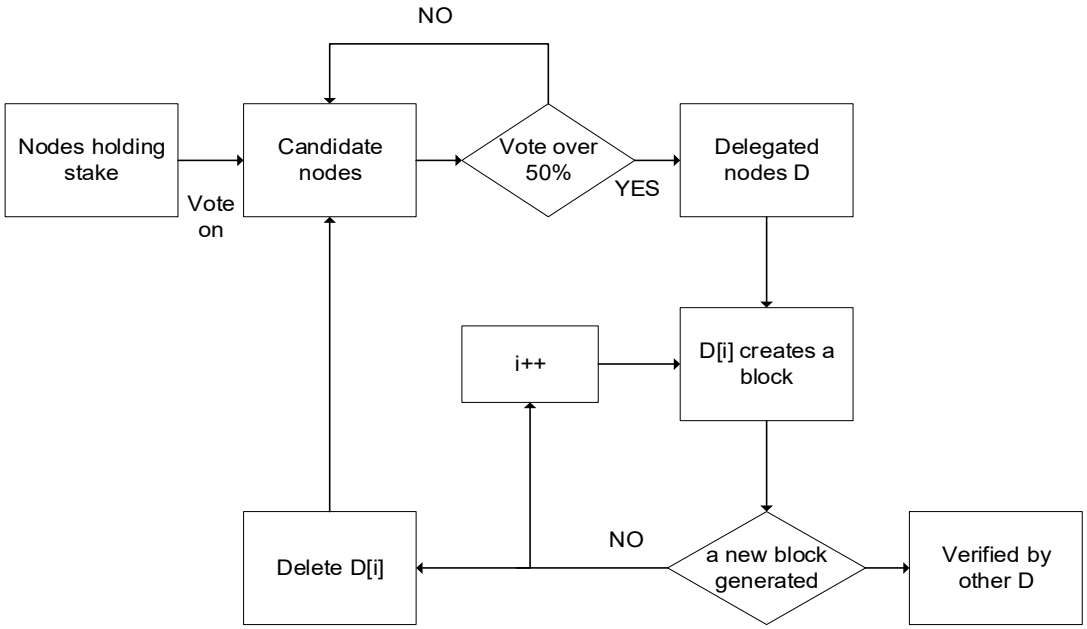


**Figure 3.** Schematic Diagram of DPoS [7]

To reduce cyber attacks caused by increased transaction rewards, Bentov et al. [8] designed the PoA consensus mechanism in 2014. It addresses the issue in PoS where some eligible participants are unwilling to engage in consensus. The principle is to involve coin holders in maintaining blockchain security: since they are less sensitive to mining rewards and more concerned with preserving and increasing the value of digital currencies, they will voluntarily maintain the network[9]. Meanwhile, rewarding highly engaged coin holders boosts their enthusiasm, with rewards determined by the specific business of platforms using the PoS algorithm.

In 2025, Wang Xinsheng et al. [10] proposed an improved DPoS scheme based on the Shapley value. This scheme optimizes the election of accounting nodes through a witness committee and a cumulative coefficient to balance consensus efficiency and decentralization; introduces

the Shapley value algorithm for the redistribution of block proceeds, and combines the proportion of voting rankings to encourage node participation; sets up a punishment mechanism to quickly eliminate malicious nodes and fills the gaps with alternative witnesses.

## 2.3. BFT Consensus Mechanism and Its Variants

BFT is a consensus mechanism used to solve node failures or malicious behaviors in distributed systems. Its core is to enable honest nodes in the network to reach a consistent decision through multi-round information interaction and voting verification even when there are some faulty nodes (including those that intentionally deceive).

The PBFT consensus mechanism was proposed by Miguel Castro and Barbara Liskov [11] in 1999, which solves the problem of low efficiency of the original Byzantine fault tolerance mechanism. As shown in Figure 4, when a client sends a request, the primary node receives it and sends the request to the replica nodes, going through three phases: pre-prepare, prepare, and commit. In the pre-prepare phase, the primary node broadcasts the request information; in the prepare phase, the replica nodes verify the message and write it into the log; in the commit phase, if the conditions are met, the request is executed. Finally, if the client receives more than f + 1 (where f is the number of Byzantine nodes, and the total number of nodes is 3f + 1) identical execution results, it is considered successful; otherwise, the view is changed and the process is repeated.

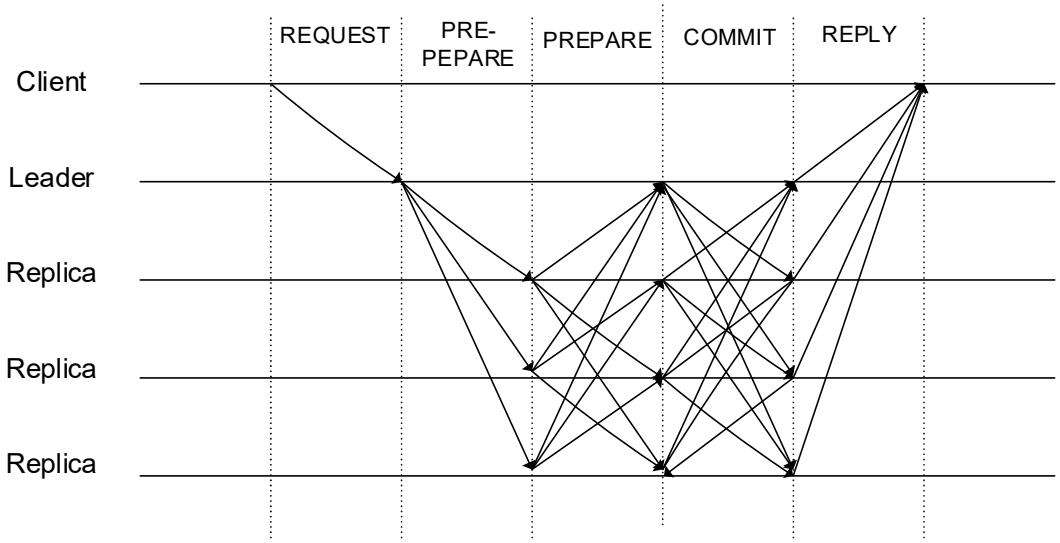


**Figure 4.** PBFT Algorithm Flowchart [9]

Delegated Byzantine Fault Tolerance (dBFT) is improved from the PBFT mechanism by Antshares Blockchain. It is designed to be more adaptable to P2P network structures. In dBFT, nodes participating in consensus can dynamically join or exit the network. The participating nodes are determined through a stake-based voting mechanism, and their real identities are authenticated with digital certificates. The working process of dBFT is as follows: Firstly, nodes broadcast transactions and record them. Secondly, the speaker sends a proposal request. Then, after receiving the proposal, the council members verify its validity and forward it. Finally, when a node receives confirmation signatures from at least ($n-f$) different council members (where n is the total number of nodes in the network and f is the number of Byzantine nodes), a consensus is reached and the complete block is published.

## 3. Comparative Analysis of Consensus Mechanisms and Existing Problems

In this section, the study will compare and analyse the performance of consensus mechanisms from the perspectives of energy consumption, degree of decentralisation, security, applicable scenarios and so on. Table 1 compares the three major types of consensus mechanisms introduced above. At the same time, due to the differences of specific consensus mechanisms under each major category, 8 typical consensus mechanisms are also selected for further comparative analysis to summarize the existing problems of mainstream consensus mechanisms, as shown in Table 2.

**Table 1.** Comparison of the Three Major Consensus Mechanisms

| | PoW Consensus Mechanism and Its Variants | PoS Consensus Mechanism and Its Variants | BFT Consensus Mechanism and Its Variants |
|---|---|---|---|
| Energy Consumption | Extremely High | Low | Low |
| Degree of Decentralization | Highest | Medium | Lowest |
| Security | Highest security | Prone to Security Vulnerabilities; Low Sercuity | Clearly Resists Byzantine Attacks (≤1/3 Malicious Nodes); Lower Security |
| Attack method | 51% Attack, Double Spending Attack, Selfish Mining; | Nothing at Stake Attack, Long Range Attack, | Leader Compromise Attack, Sybil Attack |
| Finality | No | No | Yes |
| Presence of Tokens | No | Yes | No |
| Applicable Scenarios | Public Blockchains (Value Storage) | Public Blockchains (Ecological Applications) | Consortium Chains/Private Chains (Institutional Collaboation) |
| Typical Cases | BItcoin, Litecoin | Ethereum, Cardano | Hyperledger, Fabric, Ripple |

**Table 2**. Comparison of Several Typical Consensus Mechanisms

| | PoW | Bitcoin-NG | PoS | DPoS | PBFT | dBFT |
|---|---|---|---|---|---|---|
| Energy Consumption | Extremely High | High | Low(server poeration) | Low | Low | Low |
| Degree of Decentralization | Highest | High | High | Medium | Low | Extremely Low |
| Security | Highest | Extremely High; | Low | Low | Lower | Lower |
| Forking | Prone to Forking | Prone to Forking | Yes | Yes | No | No |
| Finality | No | No | No | No | No | No |
| Presence of Tokens | No | No | Yes | Yes | No | No |

First is the Energy Consumption Issue. Consensus mechanisms represented by PoW compete for accounting rights through competition in computing power, which consumes huge amounts

of energy. Moreover, the computational power is used for meaningless hash calculations, resulting in significant waste.

Second is the Conflict Between Efficiency and Decentralization. Many consensus mechanisms struggle to balance efficient processing and decentralization. For example, Bitcoin's PoW ensures decentralization and security but has a slow transaction processing speed (approximately 7 transactions per second), making it difficult to meet the needs of high-frequency application scenarios.

Third is Insufficient Scalability. Some mechanisms experience a significant decline in performance when the number of nodes increases or transaction volumes grow, and the delay in reaching consensus may increase substantially.

Fourth is Imbalanced Incentive Mechanisms. The incentive design of some consensus mechanisms is unreasonable, which may lead to insufficient participation enthusiasm of nodes or excessive pursuit of short-term interests while ignoring the long-term stability of the network, affecting the sustainability of consensus.

## 4. Conclusion

As the core of blockchain technology, the consensus mechanism is a key support for achieving data consistency among distributed nodes and ensuring system security and efficiency. This study focuses on the analysis of typical blockchain consensus mechanisms, sorts out the principles, advantages, and defects of three major categories of mechanisms PoW, PoS, and BFT and their variants, compares them from dimensions such as energy consumption, degree of decentralization, security, consistency, and applicable scenarios, and identifies the challenges faced by current consensus mechanisms.

Through the analysis of existing consensus mechanisms, future consensus mechanisms can be optimized and designed from the following perspectives:

(1) To address the high energy consumption of PoW, can future improvements reduce energy consumption through algorithm optimizations (such as introducing effective computational power calculations instead of meaningless hash calculations) and adaptation to clean energy?

(2) To cope with the performance pressure brought by the growth of node scale and transaction volume, can consensus mechanisms use sharding technology and Directed Acyclic Graph (DAG) technology to improve system throughput through parallel processing and load distribution?

(3) Different application scenarios have significant differences in requirements for consensus mechanisms (e.g., financial scenarios require high security and finality, while IoT scenarios require low latency and lightweight computing). In the future, consensus mechanisms will develop towards "scenario-specific customization", supporting dynamic adjustment of consensus rules based on node scale, business requirements, and other factors.

(4) A single consensus mechanism is difficult to meet the requirements of decentralization, security, efficiency, and scalability at the same time. Hybrid consensus will become an important exploration direction. For example, combining the security of PoW with the efficiency of PBFT to achieve complementary advantages.

## References


[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Available at SSRN 3440802, 2008.

[2] Junk C. Pricing via Processing[C]//Advances in Cryptology-CRYPTO'92: 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16–20, 1992. Proceedings. Springer, 2003, 740: 139.

[3] Sompolinsky Y, Zohar A. Secure high-rate transaction processing in bitcoin[C]//International conference on financial cryptography and data security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015: 507-527.

[4] Eyal I, Gencer A E, Sirer E G, et al. {Bitcoin-NG}: A scalable blockchain protocol[C]//13th USENIX symposium on networked systems design and implementation (NSDI 16). 2016: 45-59.

[5] Tan Minsheng, Xu Guoqing, Ding Lin, etc Improvement of Blockchain Consensus Mechanism Based on POW [J]. Computer Applications and Software, 2024, 41 (11): 117-122

[6] Quantum Mechanic. Proof of stake[EB/OL].(2011-07-11)[2018-09-30].https://bitcointalk.org/index.php?topic=27787

[7] Schuh F, Larimer D. Bitshares 2.0: Financial smart contract platform[J]. Bitshares Financ. Platf, 2015, 12.

[8] Bentov, Iddo, et al. "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y." ACM SIGMETRICS Performance Evaluation Review 42.3 (2014): 34-37.

[9] Liu Mingxi, Gan Guohua, Cheng Yukun, etc The Development Status and Prospects of Blockchain Consensus Mechanisms [J]. Journal of Operations Research, 2020, 24 (1): 23-39

[10] Wang Xinsheng, Jiang Liwei, Xiong Shuming Improved DPOS consensus mechanism based on Shapley value [J]. Computer Applications and Software, 2025, 42 (1): 234-240

[11] Castro M, Liskov B. Practical byzantine fault tolerance[C]//OsDI. 1999, 99(1999): 173-186.