MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

ODESSA I.I. Mechnikov NATIONAL UNIVERSITY
(full name of higher education institution)

Faculty of mathematics, physics and information technologies
(full name of the institute, name of the faculty)

Department of mathematical support of computer systems
(full name of the department)

# Qualification work

for obtaining the "master" higher education degree
(education level)

on the topic "Optimizing data security and stability of blockchain technology in the global value exchange system"

Performed by: a full-time student of the
specialty 126 – Information Systems & Technologies
(specialty code and name)
educational program «Information Systems & Technologies»
(educational program name)
HE JI (Anonymized)
(Full Name)

Scientific supervisor Ph.D., Assoc. Prof. Antonenko O.S.
(academic degree, academic title, surname and initials, signature)

Reviewer _____
(academic degree, academic title, surname and initials)

Reviewer _____
(academic degree, academic title, surname and initials)

Recommended for defense:
Minutes of the department meeting
No.___ of "___"_____ 2023

Head of Department
_____ E.V. Malakhov
(signature) (surname, initials)

Defended at the EC No. ___ meeting
Minutes No. __ of "___" _____ 2023
Score _____/____/_____
(by national scale, ECTS scale, points)
Chairman of the EC
_____ V.V. Vychuzhanin
(signature)
(surname, initials)

Odesa - 2023

Abstrack

The "blockchain" technology has gradually entered the lives of the public and become the focus of attention in society. Blockchain originated from Bitcoin and utilizes an encrypted chain blockchain structure to store data. Consensus algorithm is a core issue in blockchain technology. Using consensus algorithm to generate and validate data can effectively solve the problem of reliable transmission of trust and value on the Internet.However, in the value exchange system, blockchain has never truly been resolved and has achieved sufficient security. If its security and efficiency can be improved, it will greatly strengthen the fundamental tool effect in the global value exchange system

**Keywords: Blockchain;Identification algorithm; Encryption technology**

**CONTENT**

## 1.1 **Background description of blockchain research field**:

The value exchange system of blockchain technology is a computer protocol aimed at disseminating, validating, or executing contracts in an information-based manner. The most classic of these is that smart contracts allow for trustworthy transactions without a third party, which are traceable and irreversible. The purpose of smart contracts is to provide a secure method that is superior to traditional contracts and reduce other transaction costs associated with the contract. A smart contract is a set of commitments defined in numerical form, including protocols on which contract participants can execute these commitments.

Due to the many advantages of using blockchain technology in value exchange systems. The advantages include decentralization, timestamp and irreversibility, openness, and convenience in the entertainment consumption system, while customer consumption and entertainment come with a point effect. Blockchain technology is applied in value exchange systems, such as service exchange, commercial value exchange, and currency attribute value exchange. From a commercial perspective, such systems come with inherent traffic and dissemination attributes, but from a technical implementation perspective, there are still many hidden dangers and drawbacks. Currently, there is no globally recognized trading currency in the game system

## 1.2 Main issues:

Blockchain technology is applied in value exchange systems, such as service exchange, commercial value exchange, and currency attribute value exchange. The problem with the exchange of monetary attribute value is that the computational complexity is enormous, and the security of monetary attribute value exchange has always been a concern For example, in 2014, the MT GOX was stolen with a total of 750000 Bitcoins, leading to the closure of the exchange. Although the hierarchical and layered design of blockchain computing and communication systems is perfect, the technology of sharding design is still not perfect. It can lead to a lack of response time and stability of computing nodes during the execution of concurrent tasks with huge computational load. The biggest

advantage in blockchain technology 1.0 and 2.0 has become a systemic weakness in the later stages of development.

### 1.3 Research objectives:

Optimize the storage security and address algorithm redundancy in the blockchain value exchange system, and improve the operational efficiency and security of system nodes in the face of concurrent big data.

### 1.4 **The main tasks that need to be addressed to achieve the objectives of this study are**:

Strengthen the security of the value exchange system from the perspective of key or encryption algorithms in the underlying design, enhance the security of the blockchain value exchange system from the perspective of information storage methods, and adopt optimization algorithms or replace old computing models with new mathematical models from the perspective of saving computing resources for blockchain nodes. Fundamentally solve the security issues of storage and value exchange from the perspective of algorithms or methods. Secondary tasks include the expectation of achieving inherent value independence in the trading system, such as value exchange reflected in human social services

### 1.5 Characteristics of blockchain:

Blockchain has the characteristic of decentralization, indicating that it no longer relies mainly on central nodes and implements a distributed recording method for data, while storing and updating data. In traditional networks, with centralization as the technical feature, business execution relies on the credibility and robustness of the central node. In blockchain, the distributed structure of blockchain

Construct a uniform distribution of nodes across the entire network, and the data in the system is jointly maintained by the entire network. All public nodes in the blockchain are open, and any node can access them through public access

The interface is open for data queries or application development, and the entire system is open. In a blockchain system, all data related to publicly available nodes can be accessed,

Elaborate and analyze the basic principles of POW, POS, DPOS, and PBFT consensus algorithms, and analyze some of their shortcomings. The consensus algorithm is a key technology in blockchain technology, playing a decisive role in blockchain security, efficiency, and other aspects. It determines the generation rules of blocks in the blockchain, and commonly used consensus algorithms include POW

POS, DPOS, PBFT.

Keywords: blockchain; Algorithm recognition; Encryption technology

Figure 1: Blockchain structure

Figure 2: Proof of Work Process

Figure 3: Execution process of Byzantine fault-tolerant algorithm 153

But the private information at the delivery date is encrypted through a hash function, so data exchange and transactions are conducted anonymously. Blockchain technology uses two sets of encryption techniques to prevent records in the blockchain from being tampered with

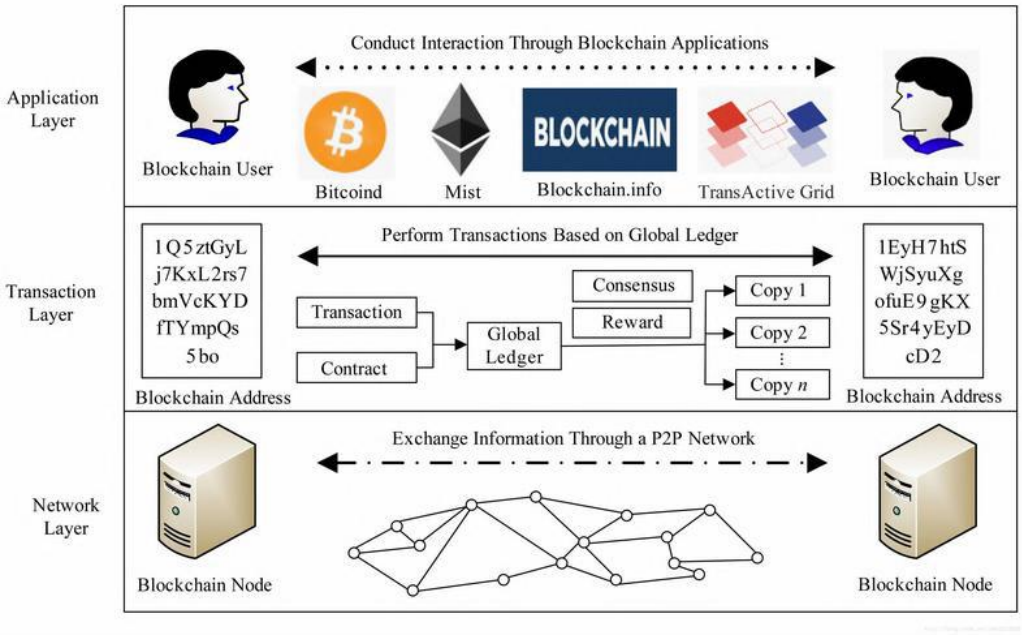


Figure 1: Blockchain structure

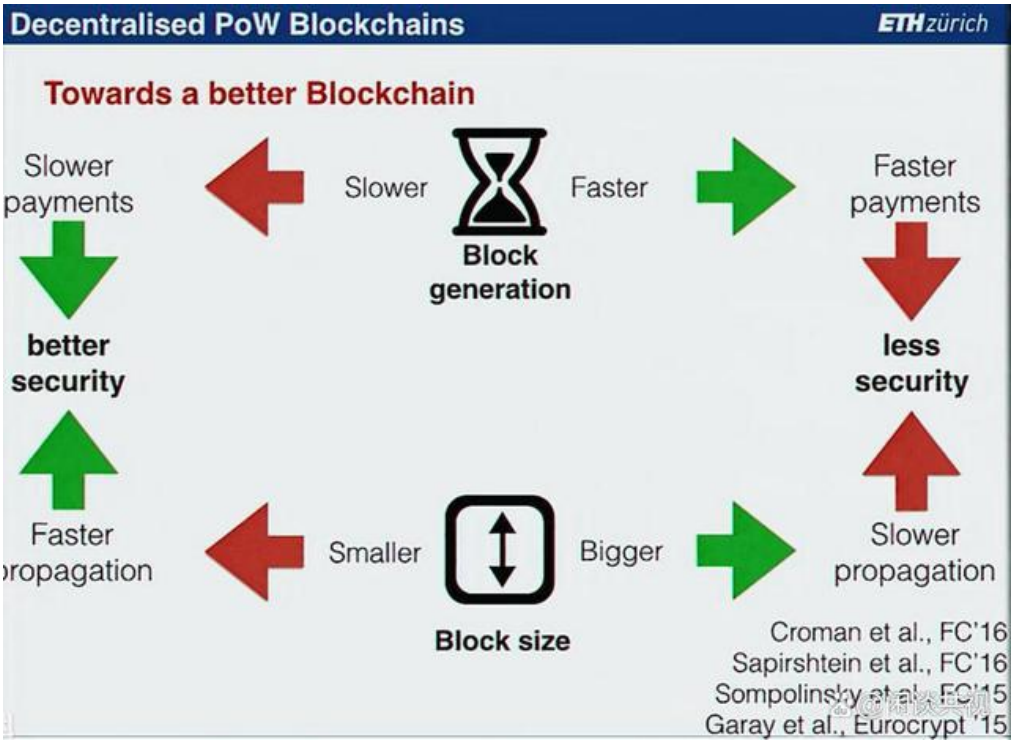


Figure 2: Proof of Work Process

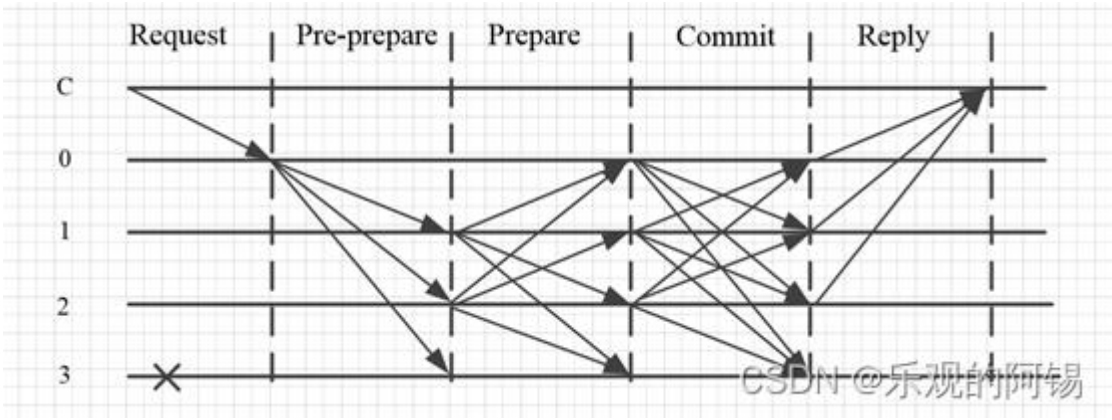


Figure 3: Execution process of Byzantine fault-tolerant algorithm 153

Change. One set is recorded using the Merkel tree method; Another approach is to place a hash value before creating a new block. These two encryption mechanisms make the data in the blockchain highly stable and reliable. From the perspective of the openness of blockchain, it can be divided into consortium chain, private chain, and public chain. As shown in Figure 1, each chain contains different algorithms, and this article mainly studies the common chain in consensus algorithms. With the continuous development of

blockchain technology, the boundaries between each type of chain in the blockchain will also become blurred. As the smart contracts running on nodes become increasingly complex, some nodes on the private chain must be open to execute corresponding business logic, while some consensus nodes only guarantee their openness to the licensed nodes, and the business boundaries between chains will gradually become blurred.

## 2. Advantages and disadvantages of existing methods/algorithms/IT for solving the same problem:

Currently, blockchain systems have 9 major categories of algorithms from a philosophical perspective

Core methods or algorithms of blockchain

### 2.1 Byzantine Agreement：

Advantages: Most physical computing nodes are benign, and the value and security of data are excellent.

Disadvantage: If the attacker, such as a technical hacker, can control and modify more than half of the nodes, security will be compromised. Although this probability is low, the cumulative number of dangers that have already occurred is also astonishing.

### 2.2 Asymmetric encryption technology

Advantages: Two different keys are used for encryption and decryption in asymmetric encryption algorithms. Paired keys are difficult for disruptors to simultaneously crack.Normative irreversibility. Non Breach of Contract. Anonymity.Disadvantage: If one of them is destroyed, it will result in significant damage in reverse computing.

### 2.3 Fault tolerance issues

Advantages: Nodes can act arbitrarily on information, including loss, damage, delay, and duplicate sending. The order of receiving and sending is inconsistent, and the algorithm includes security and availability applicable to any network environment.

Disadvantage: Fault tolerance may be used by special protocols to disrupt and modify information behavior. For example, when the physical reason loses transmission blocking or delay, ports with the same information slope can forge some information in advance and modify the content after this delay period, because at this time, node computation and transmission are in a dual channel blocking state. Although this behavior is also difficult to implement, it exists logically and methodically.

### 2.4 Paxos algorithm (consistency algorithm)

Advantages: Execute consistency algorithms on each node to ensure consistency of commands seen by each node. One important issue in distributed computing is multi scenario, which is a crucial issue in distributed computing. There are two modes of node communication: shared memory and information transmission.

Disadvantages: Due to the model of the algorithm itself, the speed is poor, and if information is stolen in physical communication mode, there is a possibility of tampering with the information.

### 2.5 Consensus mechanism

Advantages: In Bitcoin's consensus algorithm, the main focus is on proof of workload and proof of equity, and the algorithm Hashcash is reused to generate results that reflect value.

Disadvantage: The execution process can be monitored, but the value endorsement in the early stage of execution requires cost consumption, including a significant amount of computational power endorsement or the exchange process of physical value in real society. The later value of a system like Bitcoin comes from its meaningless consumption of computing power. We should have or invent a more advanced system for replacing real values.

### 2.6 Hash algorithm

The hash functions used in the Bitcoin system are used to perform workload proof calculations and generate addresses. In short, the hash algorithm maps any length string to a shorter fixed length string. Due to the certainty and efficiency of this operation,

decentralized computing can be achieved. Due to the sensitivity to input and the difficulty in finding the inverse function of the mapping (such as antigen attacks), it greatly contributes to the security of blockchain systems.

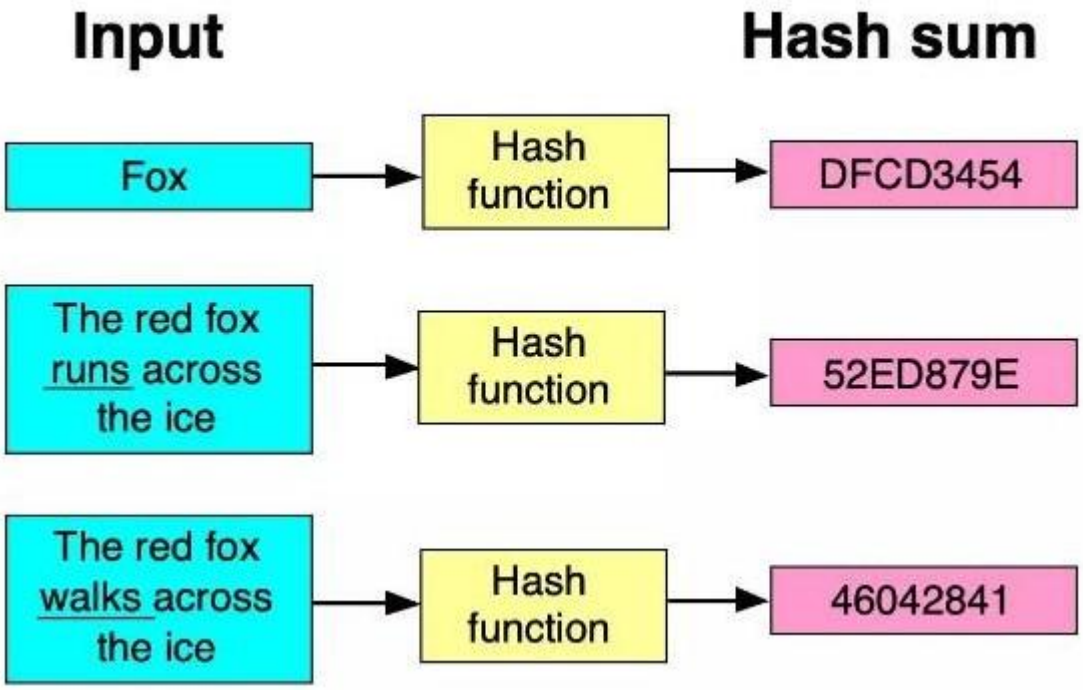


Figure 4: Hash algorithm

## 2.7 Elliptic curve algorithm

Elliptic curves are a set of algorithms for encrypting data, decrypting data, and exchanging keys, which can also be used for data signature and verification.

Signing can ensure that the user's account is not replaced by others, and on the other hand, it ensures that the user cannot deny the transaction they have signed. Sign the transaction information with a private key, and the miner verifies the signature with the user's public key. If the verification is successful, the transaction information is recorded and the transaction is completed.

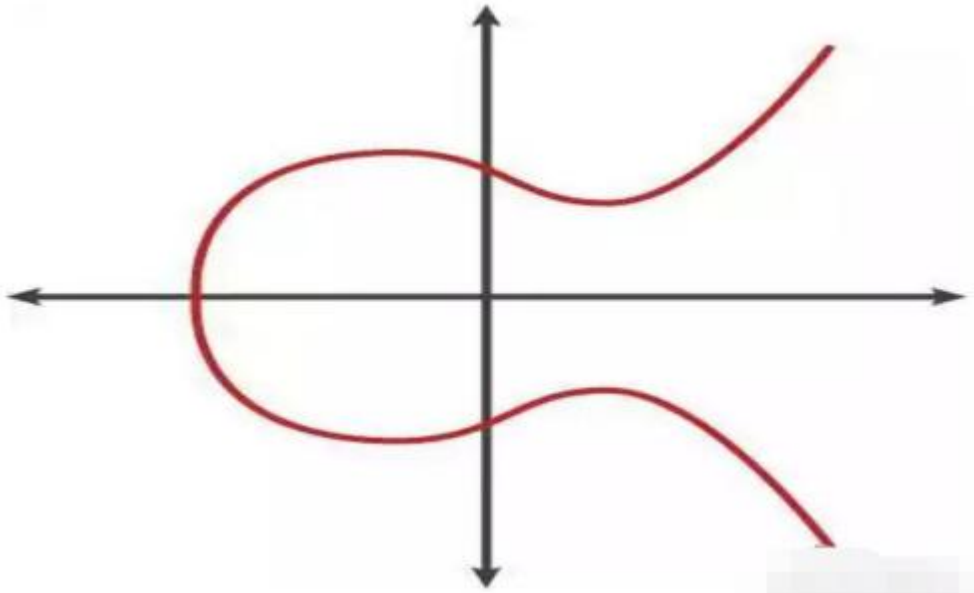

Figure 5: Elliptic curve algorithm trajectory diagram

## 2.8 Base58 encoding

Base58 is the encoding method used by Bitcoin, mainly used to generate wallet addresses for Bitcoin. This encoding format not only achieves data compression, maintains readability, but also has error diagnosis function.

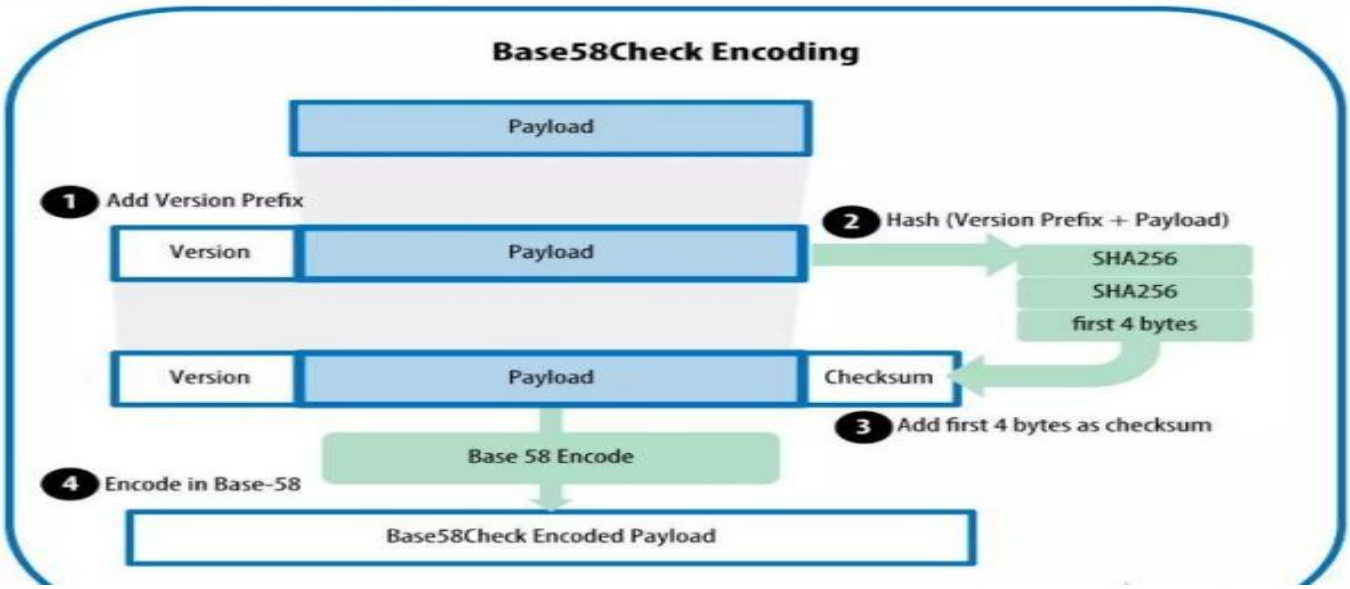


Figure 6: Base58 encoding flow path

## 2.9 Zero knowledge proof

Zero knowledge proof is a technology jointly proposed by computer scientists Goldwasser and Micali in the early 1980s. It mainly refers to the ability of the verifier to make the verifier believe that a certain statement is correct without providing any useful information to the verifier.

Zero knowledge proof requires three elements to be established, namely completeness,

reliability, and zero knowledge. For example, suppose there is a circular corridor where the exit and entrance are adjacent but not interconnected (within a visual distance), and there is a locked door in the middle of this circular corridor that only those with keys can pass through; At this point, A needs to prove to B that he has the key to open this door, using zero knowledge proof to solve the problem. B watches A enter the entrance and wait at the exit. If A enters through the corridor from the entrance and exits, it can prove that he has the key to open the middle door. In this process, he does not need to provide specific information about the key to B. So zero knowledge proof is actually a probability proof rather than a deterministic proof.

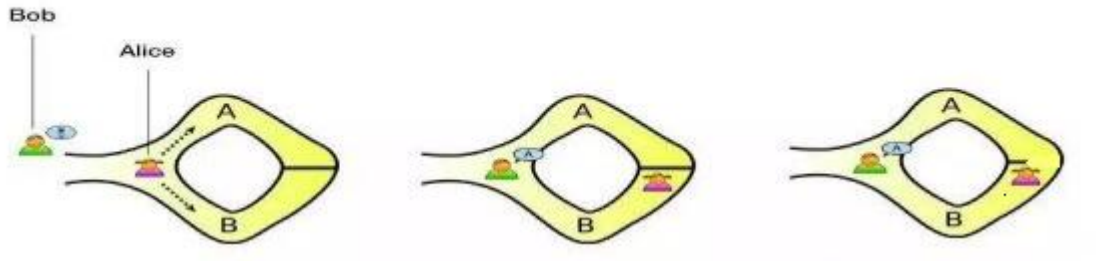


Figure 7:Zero knowledge proof

### 2.10 Blockchain 1.0 Phase

In the blockchain 1.0 phase, the main feature is the use of distributed ledger technology, which is distributed

The traditional ledger technology can be seen as a means of managing multiple nodes, different geographical locations, or multiple. A network database composed of organizational structures. Blockchain 1.0 adopts a blockchain data structure,Ensure anti tampering of transaction data.

### 2.11 Blockchain 2.0 Phase

Adopting a set of digital defined commitments, automatically executed by the computer. Promised middle package .Including the rights and obligations agreed upon by contract participants, by introducing smart contracts, users are similar.Initiate a transfer transaction that requires the execution of the relevant rules of the specified contract, in order to enable the block.The chain system has evolved into a central computing platform.

Blockchain technology has been widely applied in various fields, in terms of science and technology,

Blockchain can assist many disciplines in solving scientific and technological problems,

such as blockchain+internet,Blockchain+cryptography, blockchain+finance, and so on. From the perspective of the applicability of blockchain.Blockchain adopts a distributed computing approach to achieve ledger sharing and data information sharing.By using blockchain technology, information is no longer centralized, and data information security is improved .Ensure the openness and transparency of data. So as to make the security of blockchain universal.Identification. Blockchain has rich application scenarios, and for the problem of information asymmetry, blockchain,Chain technology adopts two sets of encryption techniques, and public data can be transparently implemented.In blockchain systems, consensus algorithms play an important role. It not only assists node protection.Maintaining consistent data while also having certain functions for token issuance and attack prevention. From 2009.Since the birth of the first blockchain system in [year], with the maturity of blockchain technology, blockchain has been widely used.The recognition algorithm is also constantly developing and improving, and has evolved into various branches to this day.

With the rapid development of the blockchain industry, the security of blockchain is gradually being enhanced by blockchain technology

The importance of blockchain applications and R&D personnel, in the algorithms of blockchain technology, transactions are no longer limited.

The mechanism that revolves around the center can also ensure the consistency of data across the entire network, thus achieving point-to-point.The design of rules for these transactions is particularly important. In the research of blockchain technology.The consensus algorithm, as the core content of its technology, plays a decisive role in the use of blockchain.The role of blockchain, including security, efficiency, and other aspects.

The PBFT (Practical Byzantine Fault Tolerance) algorithm is a distributed system consensus algorithm that can tolerate Byzantine errors.

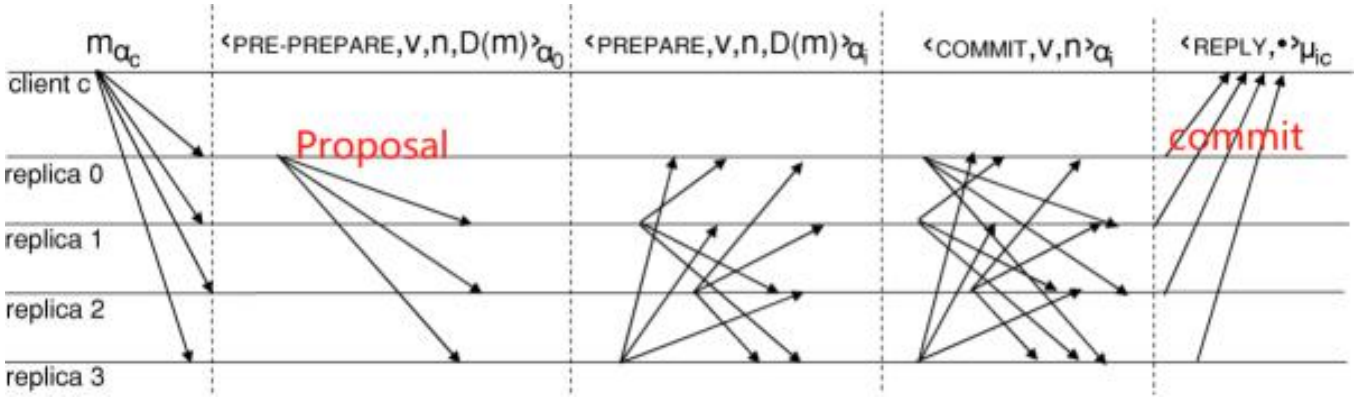


Figure 8: PBFT algorithm execution process

### 2.12. DeFi (Decentralized Finance)

DeFi is a blockchain application that allows users to conduct financial transactions and services without the need for traditional financial institutions. It includes lending, stablecoins, liquidity mining, decentralized exchanges, etc. DeFi refers to a financial system built on blockchain technology, aimed at achieving more open, transparent, and autonomous financial services. Through smart contracts and decentralized mechanisms, DeFi eliminates the intermediary links of traditional financial institutions, allowing users to directly conduct various financial transactions on the blockchain, such as lending, trading, wealth management, etc. The core concept of DeFi is to provide users with greater autonomy and higher financial efficiency.

### 2.13. NFTs (Non Homogeneous Tokens)

NFTs are blockchain based digital assets that represent unique digital items such as art, music, virtual land, and virtual items. The NFT market is growing rapidly. NFT, also known as Non Fungible Token, refers to a non-homogeneous token that is essentially a trusted digital equity credential with unique characteristics in blockchain networks. It is a data object that can record and process multidimensional and complex attributes on the blockchain.

### 2.14. Layer 2 Extension

In order to improve the performance and scalability of blockchain networks, Layer 2 solutions such as Lightning Networks and Rollups are emerging.

Cross chain interoperability: In order to achieve interoperability between different blockchains, some projects are developing cross chain solutions that enable different blockchains to communicate and exchange assets with each other.

Privacy protection: Blockchain privacy protection technologies such as Zero Knowledge proofs and homomorphic encryption play an important role in protecting user data privacy.

Programmable Blockchain: Programmable blockchain allows developers to build more complex smart contracts and decentralized applications. Ethereum 2.0 is an example that utilizes PoS (Proof of Stake) and sharding to improve performance.

Blockchain standardization: Industry organizations and international standard setting bodies are actively promoting blockchain standardization to improve interoperability, reliability, and security.

CBDCs (Central Bank Digital Currency): Some countries are researching and experimenting with central bank digital currencies, which will be issued by central banks and recorded on the blockchain.

Governance models: New governance models and DAOs (decentralized autonomous organizations) are emerging to promote community decision-making and sustainable development of networks.

Green Blockchain: Focusing on the energy consumption of blockchain, some projects are seeking more environmentally friendly consensus mechanisms and sustainable mining methods.

**2.15 Distributed Storage**

Advantages: The disk space on each machine transforms these scattered storage resources into virtual storage devices, which are difficult to destroy or modify simultaneously.
Disadvantage: Its dispersed storage reflects security and is also the biggest risk of value owners losing information.

**2.16 Proof of Stake (POS)**

In proof of equity, digital currencies have the concept of cryptocurrency age: cryptocurrency age=number of holdings × Proof of ownership for holding time encourages Bitcoin holders to increase their holding time and, through the concept of coin age, eliminates the reliance on workload calculations for blockchain proof. Meanwhile, the greater the value of blockchain, the higher its security. When attackers want to attack blockchain, they need to accumulate a large amount of coin age, which increases the difficulty of the attack and enhances the security of blockchain. In the proof of equity mechanism, the value of blockchain is directly proportional to its security.

**2.17 DPOS (Delegated Proof of Stake)**

In the previous consensus algorithm, each node could vote to select a representative based on their own shareholding rights. In the entire network, the node that participated in the vote and received the most votes will receive accounting rights. These nodes generate blocks in a predetermined order and receive corresponding rewards. In obtaining accounting rights, a node needs to pay a certain amount of security deposit and ensure a certain amount of online time. If at a certain moment it needs to generate a block and the node does not fulfill its responsibilities, the accounting rights of the node will be cancelled, and the system will continue to vote to select a new node representative to replace it.

**2.18 Byzantine Fault Tolerance Algorithm (BPFT, Delegated Proof of Stack)**

The Byzantine concept applies to views, where in each view, only one primary node needs to be defined, and all other nodes are defined as backup nodes, all of which are sent to the backup node. After receiving the sorting result, the backup node needs to check whether the request sorting sent by the master node is normal. If an exception is found, it will trigger an attempt to replace the mechanism, replacing the next numbered node as the master node. In the Byzantine fault-tolerant algorithm, the flowchart of when the client sends a request and receives a reply is shown in Figure 03

3.0 More advanced methods to solve existing problems:

3.1 Methods for Nine Major Categories

There are optimizable methods or algorithms that can improve the security and speed of blockchain in value exchange systems, addressing the shortcomings of the existing 9 categories of methods or algorithms

The algorithms and methods currently under research include:

The original password key was asymmetric encryption, but once the encryption or decryption key is obtained, these keys will all be the public key. We can divide the key into a public key and a private key in the key, which can increase the security of the key by thousands of times at a very small algorithmic cost

Distributed information storage itself has advantages and supports the definition of decentralization, while also bringing more costs to centralized verification of information. These costs include time, computing power, loss of existence, and whether it is possible to create a specialized, decentralized service under transaction premise to reduce or eliminate such errors.

In the past, early value trading systems, such as Bitcoin, were based on computing power to give birth to new value currencies in old systems. This was essentially a pointless waste. Establishing a process of directly creating equivalents between the real world and the digital world would eliminate the waste of computing power and the fallacy of generating digital system wealth out of thin air, I will temporarily name this method "Real Digital Fruit". The meaning of this method is that only the value in reality can give birth to the general equivalent of blockchain systems. The world is originally a family, and improving the value exchange system of blockchain while establishing a universal currency for global gaming or entertainment systems is also a pioneering move.

**3.2 Security and Algorithm Redundancy**

Optimize storage security and algorithm redundancy in blockchain value exchange systems, and improve the operational efficiency and security of system nodes in the face of concurrent big data.

The main tasks that need to be addressed to achieve the objectives of this study are:
Strengthen the security of the value exchange system from the key or encryption algorithm in the underlying design, enhance the security of the blockchain value exchange system from the design of information storage methods, and from the perspective of saving blockchain node computing power, adopt optimization algorithms or replace old computing models with new mathematical models. Fundamentally solve the security issues of storage and value exchange from the perspective of algorithms or methods. Secondary tasks include the expectation of achieving pure value independence within the trading system, such as value exchange reflected in human social services.

If both parties breach the contract in the transaction, the platform will automatically call the smart contract to punish the defaulting party, and its punishment rules will apply
The smart contract has been written in advance, and once a breach occurs, the penalty will be immediately executed, and the breach information will be broadcasted to the number of transactions involved
Synchronize updates based on all nodes on the chain, which will affect the user's overall reputation value and serve as a basis for future filtering consensus nodes and selecting services
Based on this, to improve the success rate and credibility of transactions

**3.3 Core ideas**

The existing BCAC algorithms can mainly be divided into using credit mechanisms to optimize existing ones.
There are two types of consensus algorithms: consensus algorithms and new consensus algorithms constructed using credit mechanisms. Below.Introduce the implementation principles of different types of consensus algorithms separately.

**3.4 Credit+Existing Consensus Algorithm**

(1) Algorithms such as Credit+PoX Consensus utilize credit mechanisms for proof classes。
The algorithm is optimized, where X can represent W in PoW or S in PoS, etc. Dian。

Reference [9] introduces credit mechanisms into PoW, which is beneficial for participating in PoW consensus

Calculate and rank the credit rating of all nodes, and solve sha256 based on the ranking。

The search space for mathematical problems is allocated proportionally to each node, and the nodes successfully solve them.

Hash puzzles will obtain miner status and corresponding rewards. Node credit value in.

The algorithm plays two roles: a) Nodes with higher credit values will receive more searches

Search for space, with a higher probability of becoming a miner node; b) Credit value is used to measure whether a node is.The basis of Byzantine nodes enhances the security of consensus algorithms. The advantages of reference [9].The key is to increase the fault tolerance of PoW algorithm's faulty nodes and better handle bifurcation problems.The question greatly increases the efficiency of the PoW algorithm. But the network size is smaller than PoW,The algorithm design is also more complex. Similarly, reference [12] focuses on nodes in the Internet of Things.Propose a blockchain based IoT system based on resource constraints and data security requirements.Unify and design a credit based PoW consensus mechanism. Credit value used to adjust PoW

The difficulty of the algorithm is reduced for honest nodes, while for malicious nodes, the difficulty is reduced

Increase the difficulty of solving. The advantage of the algorithm is the use of directed acyclic graphs

As the underlying data structure of blockchain, clicgraph (DAG) improves the system's performance

Throughput; The disadvantage is that the algorithm is essentially still solving the hash problem in PoW, especially

Especially when there are many malicious nodes in the system, the algorithm complexity is higher.

Reference [10] introduces a credit mechanism into PoS, taking into account the various nodes involved

Calculate the credit of nodes based on the number of effective blocks, effective votes,

participation, and historical credit ratings

Value, combined with the node's own rights and credit value, to select a consensus node set. node

The main role of credit value in algorithms is to select consensus node sets, and credit value

High nodes ensure the security of the PoS algorithm. The advantage of reference [10] is its ability to analyze PoS

Improvements are limited to the initial stage, such as selecting a set of accounting nodes, and addressing the complexity of PoS itself.There is not much improvement in complexity; Its disadvantage is that the utilization of credit value is not high, which can affect.

The efficiency of generating accounting nodes has not improved. Reference [13] introduces credit mechanisms.

In the DPoS consensus mechanism, credit scores and other metrics are set based on the behavior of nodes.

Level, increase the difficulty of obtaining votes for malicious nodes, and provide reward mechanisms to improve nodes.The voting enthusiasm of nodes with lower credit ratings needs to be improved in order to become witness nodes.More votes, while high credit nodes only require a small number of votes and have greater priority.

The advantage of becoming a witness node is that it has designed a system for raising and lowering the node's credit rating.The disadvantage of the reward and punishment system for participating in voting is that the assignment of node credit val.

Reference [18] designed a credit based area suitable for industrial IoT.

The blockchain consensus protocol, which allows the credit module to be ported to the current PoX consensus, proposes.The selection rules for miner nodes and the node credit reward and punishment mechanism. Its advantage is the credit model

Blocks have high portability; The disadvantage is that the selection of miner nodes still relies on high consumption.The consumption of hash operations poses a challenge for resource constrained sensor nodes. literature[19] Propose a master-slave multi chain blockchain structure, where the slave chain uses credit based PoS.Consensus mechanism,

which uses multiple consensus mechanisms in the main chain to jointly calculate and verify the method from the chain.

The generated blocks. The calculation of credit value is accumulated by the contribution of nodes when packing blocks.Calculation is mainly evaluated based on the number of completed transactions, and credit values can be used as PoS to select accounting records.

The basis and rights of the node. Its advantage is that it proposes to adopt a fusion of multiple consensus mechanisms

High security, master-slave multi chain structure to improve system throughput; The disadvantage is credit value evaluation

The factors considered are single, and the credit penalty mechanism for node wrongdoing is too strict and numerous

The integration of consensus mechanisms will inevitably bring significant time costs.

(2) Algorithms such as credit+BFT consensus utilize credit mechanisms to address BFT issues

Optimization is carried out using the algorithm, typical examples such as reference [11] based on the node's own assets and transaction.

Calculate the credit value of activities and consensus participation, and select the node with the highest credit value.As the leader node, responsible for generating blocks, new blocks are voted based on credit

Verification and confirmation, all nodes involved in the consensus process (with a credit rating ranking in the top 20%).The node will receive rewards based on the proportion of its credit value. Node credit value is being calculated

The main function of the law is to select the leader node and the voting verification node, and

Use credit value as the basis for allocating system currency. Its advantage is that the node credit value is

The allocation basis for actual currency in the system has a clear incentive effect; The disadvantage is that the nodes work together

Evil will cause negative credit values, making it difficult to participate in the credit consensus process. literature

[14] Introduce credit mechanism into BFT consensus and select node shapes with high credit values

Establish a consensus committee to reduce the probability of malicious nodes entering the committee. Built on

A credit value calculation model for machine learning, selecting node response time, equity value, and impact

Type should be used as a feature. Its advantage is to propose a node credit value based on machine learning.Computational model, supporting addition and subtraction of features, adopting a random strategy to increase entry into the committee section。

The unpredctability of points; The disadvantage is that the credit value lacks a reward and punishment mechanism, and the credit oligopoly node Easy to form.

Reference [15] designed a consensus node, candidate node, and ordinary node

A parallel hierarchical scheme composed of delegate candidate nodes to preliminarily verify the existence of transactions

Efficiency, implementing logical verification of parallel transactions in both the primary and backup nodes. Have reference from Computer Application Research Volume 40 Page322.

Consensus nodes with good performance will receive higher credit values and a higher probability of success,Become the master node and remove the faulty node from the consensus node set by setting a credit threshold.

In addition, more reliable candidate nodes will be added. Its advantage is parallel transaction validation processing.Increased throughput; The disadvantage is that it does not consider the situation where nodes are not maliciously malicious, and lacks the ability to .The mechanism for recovering from a faulty node to a consensus node effectively. Reference [17] adopts committee members

It will replace the work of a single miner node, first sorting the node's credit value,

Generate random numbers through a given distribution function to rank among the top nodes in the credit score rankings

Choose a node to join the committee, and if there are more than two-thirds of the honest sections in a round of consensus。 If clicked, the round will be successful and the credit value of each committee member will increase. No.If the honest node is less than 2/3, the protocol stops and the member's credit value is affected

To punish. Its advantage is that collective accounting avoids the risk of single node wrongdoing; The disadvantage is that

Lack of evaluation models for node credit values, overall rewards and punishments for node credit values,

Easy to cause negative behavior and insufficient motivation in some nodes. Reference [25] proposed that

A consensus algorithm based on segmented DAG and BP neural network adapted to alliance chains

Design a node credit value evaluation mechanism based on BP neural network, which is more accurate

Evaluate node credit. Design a data storage structure based on segmented DAG, improving

Improve system scalability and transaction concurrency. Its advantage is the use of BP neural network

Establish a node credit evaluation model to address the inability of linear algorithms to effectively evaluate node rows。 Describe the problem for features while optimizing the underlying storage structure to improve system throughput。 Quantity and consensus reduction experiments; The disadvantage is that the punishment mechanism for node wrongdoing is too strict,

Once there is malicious behavior, it is difficult to compete to enter the organizing committee node and leader node.Reference [28] proposes a medical blockchain consensus algorithm based on credit rating classification。

Method, calculated based on the node's participation in block consensus behavior (voting situation for blocks)

Calculate its credit value. After obtaining credit, propose self optimization based on marine predators

The credit rating classification algorithm comprehensively considers the cumulative credit, historical credit, and cost of nodes。

To represent the number of nodes and provide the number of invalid blocks. Design improvements for PBFT。

The algorithm effectively prevents malicious nodes from becoming the main node and improves consensus efficiency. Its advantages。

The new credit rating classification algorithm can effectively distinguish malicious content in the medical blockchain。 Nodes; The disadvantage is that there are too many variable parameters in the node credit value calculation model, which reduces the throughput。

Usability. Reference [30] proposes a credit based Byzantine fault-tolerant consensus algorithm, based on

Calculate the node credit based on the completion of consensus by the consensus node, and classify the node based on the credit value。 Divided into consensus nodes and candidate nodes

(3) Reference [20] proposes an application of credit+other consensus mechanisms in the automotive industry

A crowdsourcing blockchain framework for the internet, proposing a node credit model, utilizing trust propagation and anti

Calculate the credit value of the similarity calculation node and use the credit value to reveal the parameters in the connected vehicle network.Optimize the Raft algorithm's anti attack capability against any malicious behavior of nodes. Its advantages

It is a credit model that reduces the credit of any malicious service consumer or provider, effectively preventing

Ending hostile or irresponsible behavior in handling crowdsourcing tasks; The disadvantage is credit

The model and consensus mechanism are relatively isolated. Reference [23] proposes a credit based approach

Hashgraph consensus mechanism, using credit value rewards and punishments to motivate nodes to actively participate in consensus,

And proposed a leader selection algorithm based on credit rating, which increases the randomness of leader nodes

Mechanical and anti Byzantine node capabilities. Its advantage is the evaluation of node credit value

The evaluation factors are comprehensively considered, including node performance, security, activity, and Four indicators of credibility; The disadvantage is that the self setting parameters in the credit calculation formula are too large.Many, reducing versatility. Reference [29] proposes heterogeneity in blockchain for the Internet of Vehicles.Efficient consensus algorithm for nodes based on their participation in block consensus behavior.Calculate their credit value based on their participation in transaction consensus and block verification. In obtaining credit.After obtaining the value, it is proposed to use fuzzy C-means clustering to achieve credit rating classification for heterogeneous nodes.Taking into account the cumulative credit, offline frequency, offline time, and joining trustworthiness of nodes.The number of times a list is allowed and the number of times an invalid block is provided. Ripple consensus algorithm for design improvement,Effectively avoiding the impact of malicious nodes on consensus and improving consensus efficiency. Its advantages， Randomly selecting the node with the highest credit rating as the miner node greatly enhances consensus。

Efficiency; The disadvantage is that there is not enough incentive for nodes with low credit ratings, making it difficult to become miners， Nodes can easily lead to credit oligopolies

### 3.5 Pure Credit Consensus Algorithm

This type of algorithm utilizes the credit value of nodes to redesign a new consensus mechanism, rooted in

Evaluate the credit value based on the performance behavior of nodes in the system, and

then evaluate the credit value of nodes based on their performance behavior.
Select the accounting node to generate blocks, and finally store them on the chain through block verification. Literature.
[16] Let a group of nodes with credit values higher than the set threshold take turns becoming mining nodes,
And a set of randomly selected supervision nodes supervise the behavior of miners and provide corresponding measures.
Credit score, when the miner's credit score is below the system threshold, they will be expelled from the mine
Work node set. The higher the network maturity and credit value of a node, the more it becomes a miner node
The priority is higher. Its advantages include the generation, verification, and credit of mining nodes for blocks
The values are all saved by some nodes, reducing the communication complexity of the system; The disadvantage is that miners
The credit value evaluation model for nodes is lacking, and the selection of miner nodes in each round is predictable,
Easy to cause safety hazards. Reference [21] proposes a cumulative signal for vehicle networking
The blockchain consensus mechanism of Ren Zheng first calculates the cumulative credit value of nodes and selects. Choose the node with the highest credit value as the miner node. Its advantage is based on the node
Punish credit values based on the type or severity of malicious behavior, and tolerate node behavior
Non malicious erroneous behavior; The disadvantage is that the selection mechanism for miner nodes lacks randomness,Has safety hazards. Reference [22] proposes a credit consensus algorithm suitable for consortium chains The credit evaluation index is based on the transactions contained in the effective blocks successfully generated by nodes
Number, time taken for successful chain connection, and number of invalid blocks. Designed in multiple rounds
Miner node selection mechanism, using a random algorithm for mining node selection in

the first round
Select, select miner nodes based on credit values in other rounds. The advantage is to propose
Established a relatively complete node credit evaluation mechanism, storage mechanism, and credit based miner
Node selection mechanism; The disadvantage is that the selection of mining nodes is entirely based on their credit value.Poor completeness, without considering the possibility of being a miner even in the event of node wrongdoing.
References [24, 26] all proposed a credit based consensus model, which is described in sections
Calculate the credit value of a node based on its participation in transactions, and select the node with the highest global credit value
For the miner node. The advantage of the method is that it provides a state machine model for the credit consensus model
Type, making the consensus model more universal and scalable; The disadvantage is that nodes
The evaluation of credit value only considers the number of transactions processed. Reference [27] proposes a method based on information
Designed a credit value calculation module for nodes using the semi fragile alliance chain consensus algorithm in space.Type, and allocate credit space based on the credit value of nodes, and then collect data in the credit space
Using a random algorithm to select mining nodes, nodes with a larger credit space have a greater probability of success,For the miner node, while maintaining incentives, fairness is also taken into consideration. Additionally, based on the node,A graded punishment mechanism has been designed to prevent intentional wrongdoing. Its advantage is the selection of miner nodes
While maintaining credit incentives, fairness is also taken into account, and the semi fragile hierarchical punishment mechanism is sufficient
Considering the unintentional behavior of nodes in actual networks; Its disadvantage is the use of
The linear formula for calculating node credit values is incomplete, and the evaluation

indicators are not comprehensive

### 3.6 Credit Calculation Model

The key link of the BCAC algorithm is the calculation and management of node credit values

Based on the existing algorithm evaluation indicators, this article provides a general method for calculating node credit Model.

1) Credit value evaluation mechanism

The credit value evaluation of nodes can be described as follows:

$$Ci=F(Ti) \quad (1)$$

Among them, Ci represents the credit value of node i; F is the credit value calculation function, which can be expressed as

Linear calculation formulas or neural network training functions; Ti represents node i participating in system behavior

The feature vector Ti can be represented as

$$\boldsymbol{T}_i = [\, i_{type}, i_{PN}, i_{FN}, i_{PT}, i_{AT} \,] \quad (2)$$

Among them, ittype represents the type of node i participating in system behavior, which is divided into generating blocks

There are three scenarios for verification and synchronization, among which generating blocks yields the highest credit value, only

The minimum credit value obtained by completing data synchronization; IPN handles transactions correctly for node i

Number; IFN is the number of transactions processed with errors; IPT represents the time spent processing transactions for node i;

IAT is the active time of node i in the system; The larger the iPN node, the more credit rewards it receives

The larger the iFN, the greater the credit penalty the node will face; IPT and iAT with node credit

Reference form Issue 2 Liu Huiwen, et al.: Comparative Study of Credit Based Blockchain Consensus Algorithms Page 325

The rewards are inversely proportional and directly proportional.

2) Credit value storage and update mechanism

Selecting miner nodes or measuring nodes based on node credit values in credit consensus algorithms

The important basis for point credibility needs to be stored on the chain like transaction data, which is crucial

The credit value update of points also needs to be verified by the nodes on the chain to avoid targeting node credit

Attack with value. The update of credit value can be carried out after a round of consensus is completed, and the calculation is common

The formula is represented as

$$C_i^h = C_i^{h-1} + C_i \tag{3}$$

Among them: Ch-1

I is the credit value of node i in the h-1 round. Total credit of node i

The value can be expressed as

$$C_i^{Total} = \sum_{h=1}^{H} C_i^h \tag{4}$$

Among them: CTotal

I is the total credit value of node i; H is the total round of consensus participation for node i

Secondary. The total credit value of a node can serve as the basis for the distribution of benefits in the blockchain system.

1.4 BCAC evaluation indicators

The main consideration here is the quantifiable evaluation indicators of the credit consensus algorithm, which mainly include

Throughput, latency, degree of decentralization, and security. The degree of decentralization is determined by

The probability of a node being selected as a miner node is measured, and the security is determined by the probability of malicious nodes being evicted

Measurement. Below is a quantitative formula for performance evaluation indicators.

1) Throughput is calculated by the total number of transactions processed by the system per unit of time

Calculate, the formula is

$$Throughput = \frac{\sum_{i=1}^{N} Trans\_num_i}{Time} \quad (5)$$

Among them: N represents the total number of nodes in the blockchain; Trans_numi is processed for node i

The number of transactions; Time is the running time of the blockchain system.

2) Delay refers to the time required for a round of consensus in a blockchain system,

From transaction initiation to final blockchain storage

$$delay = Time_{end} - Time_{start} \quad (6)$$

Degree of district centralization

$$P_{i\_leader} = \frac{\sum_{h=1}^{H} lead\_num_i^h}{H} \times 100\% \quad (7)$$

3) Safety ： Number of times node i has committed evil in H rotation

If there are instances of wrongdoing, it is 1; otherwise, it is 0

$$P_{Ei} = \frac{\sum_{h=1}^{H} Evil\_num_i^h}{N_E} \times 100\% \quad (8)$$

### 3.7 Qualitative analysis

Firstly, conduct a qualitative analysis of the 18 credit consensus algorithms listed in befor Figure .

From the adoption of basic consensus algorithms, underlying topology, credit value calculation methods, and throughput， Quantity, latency, degree of decentralization, security, reward and punishment mechanisms, scalability, and application field， A qualitative comparison was conducted on 10 aspects of the scenery, and the results are shown in Table 1.

Qualitative analysis method of credit consensus

| Algorithm category | Name | Basic consensus algorithm | Underlying topology | Credit value calculation method | hroughput | TIME EXTENSION | Centralization degree | safety | Reward and punishment mechanism | Scalability |
|---|---|---|---|---|---|---|---|---|---|---|
| Credit+existing consensus algorithm | CPOW[9] | pow | LINK | machine learning | Lower | HiGHer | HIGH | HIGH | None | Lower |
| | Blot[12] | pow | DAG | linear | High | HiGHer | HIGH | HIGH | Exit | Lower |
| | Povt[10] | Dpos | LINK | linear | HIGHER | HiGHer | low | HIGH | Exit | HIGH |
| | Cdpos[13] | pox | LINK | linear | HIGHER | HiGHer | low | HIGH | Exit | Lower |
| | Porx[18] | pos | LINK | linear | HIGHER | HiGHer | HIGH | low | None | Lower |
| | Cpos[19] | BFT | LINK | linear | HIGHER | HiGHer | HIGH | low | None | HIGH |
| | Por[11] | BFT | LINK | linear | HIGHER | HiGHer | HIGH | HIGH | Exit | HIGH |
| | CGR_BFT[14] | BFT | LINK | machine learning | HIGHER | HiGHer | low | HIGH | Exit | HIGH |
| | DHBFT[15] | BFT | LINK | linear | High | HiGHer | low | low | None | Lower |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | RECON[17] | BFT | LINK | linear | HIGHER | HiGHer | low | low | None | Lower |
| | Cabp[25] | BFT | GAG | machine learning | High | HiGHer | HIGH | low | Exit | Lower |
| | Sca_md[28] | BFT | LINK | linear | HIGHER | HiGHer | HIGH | low | None | HIGH |
| Pure Credit Consensus Algorithm | BRBC[16] | NONE | LINK | linear | HIGHER | lesser | low | HIGH | None | Lower |
| | POAC[24] | NONE | LINK | linear | HIGHER | lesser | low | HIGH | Exit | HIGH |
| | CCAC[22] | NONE | LINK | linear | HIGHER | lesser | HIGH | low | Exit | HIGH |
| | FRCM[24] | NONE | LINK | linear | HIGHER | lesser | HIGH | low | Exit | Lower |
| | Rcf[26] | NONE | LINK | linear | HIGHER | lesser | HIGH | low | Exit | HIGH |
| | SCACS[27] | NONE | LINK | linear | HIGHER | lesser | low | low | Exit | HIGH |

Table 1 Comparison of Qualitative Analysis Methods for Credit Consensus:

The basic consensus algorithm used usually determines the throughput, latency, and resolution of the algorithm

The degree of centralization and application scenarios, such as references [9, 18], are all based on the PoW consensus

Improvement, lower throughput, although the basic consensus algorithm in reference [12] is also PoW,

However, due to the adoption of DAG's underlying topology, parallel processing of transactions results in increased throughput

Higher. In terms of latency, the introduction of credit mechanisms in references [9, 12, 18] only reduces

The difficulty of solving problems with low credit value and high nodes is essentially solving the hash problem

Compared to other methods, the delay is relatively large. Credit consensus mechanism based on PoW, de centering,

High degree of internalization, usually suitable for public chains. Based on the PoS credit consensus mechanism,

The delay is usually small because the credit mechanism accelerates the generation of voting node sets, but

Xian [19] Due to the use of multiple consensus mechanisms in the main chain to jointly calculate methods for verification,The blocks generated from the chain have significant latency. Consensus algorithm based on BFT class,Usually has lower latency, as only nodes with high credit values can enter consensus

Node sets, even leader nodes, have a low degree of decentralization and are generally suitable for linking

Alliance Chain. From the data in Table 1, it can be seen that using DAG as the underlying data topology

Reference form Computer Application Research Volume 40 page325

The consensus method has the highest throughput, although reference [15] also uses transmission

Unified chain method, but due to the addition of parallel transaction processing mechanism, it also has high

Throughput. In general, consensus algorithms designed with credit reward and punishment mechanisms have better performance

Good scalability. The pure credit consensus algorithm utilizes node credit values to redesign the consensus

The recognition process and credit value as the sole basis for selecting mining nodes greatly accelerate the process

The recognition process has smaller latency and higher throughput.

**3.8 Quantitative analysis**

In order to better compare the performance of different credit consensus algorithms, this article adopts a unified approach. The experimental platform (CentOS operating system and node container were selected as the experimental environment)

Docker, programming language Python, frameworks PyTorch and Flask. Using Python

Write consensus algorithms with PyTorch, use Flask to write web program interfaces, and leverage

Load web program simulation nodes using Docker containers and use Alibaba Cloud

servers to

Simulate multi machine and multi node stress testing for quantitative comparative analysis. Experimental subjects。 Select credit+PoX consensus algorithms CPoW and CPoS, as well as credit+BFT consensus algorithms

Algorithm Recon and CABP, Credit+Other Consensus Algorithm ECCA, Pure Credit Class

Identify algorithms CCAC and SCACS. During the experimental process, the selected literature was compared with the actual results

Construct a three-layer BP neural network using the same parameters in the CPoW algorithm,

The mining difficulty is set to the top 5 0 prefixes of the hash value.

**(1) Throughput experiment results**

This article sets the concurrency to 300 transactions per second, and the throughput comparison experiment is shown in Figure 2

Show. From Figure 2, it can be seen that the throughput of the seven consensus algorithms varies with the number of nodes,Increased, all showing a downward trend, with literature [22, 25, 27, 29] showing stable swallowing behavior,Vomiting volume. Pure credit consensus algorithms have higher throughput and CCAC computation,The throughput of the method is higher than that of the SCACS algorithm because the latter has a higher impact on node credit,The value calculation is more complex, and credit space is used to randomly generate miner nodes,Compared to the CCAC algorithm, which directly uses credit value sorting to generate miner nodes, it is more complex,Miscellaneous, under the same transaction concurrency, the time required to complete consensus is longer,So the throughput is lower. Compared to pure credit algorithms, the throughput of credit+other consensus algorithms

The consensus algorithm is lower, depending on the consensus protocol used, due to the use of traditional chain based algorithms

Structure and throughput remain bottlenecks. The consensus algorithm of credit+PoX class has the lowest

The throughput, where CPoW allows all nodes to participate in the competition to solve

the hash problem

Although the introduction of credit mechanisms has significantly improved the throughput of the original Bitcoin system

Quantity, but still difficult to apply to practical scenarios. In contrast, CPoS has higher performance

Throughput, but the introduction of credit mechanisms only ensures that voting nodes have higher throughput

Reliability, without substantial improvement to PoS consensus, algorithm throughput needs to be improved

Significantly smaller than pure credit consensus classes. Credit+BFT algorithms with fewer nodes

At 100, it has a high throughput, but as the node size increases, reference [17]

The throughput has significantly decreased because only the election method of the leader node has been modified, and

There is no optimization of traditional PBFT in terms of performance, so as the number of nodes increases, it will cause,The sharp increase in communication volume has led to a sharp decline in TPS. And literature [25] adopts,Using DAG as the underlying storage structure for data and utilizing MapReduce to improve transactions,Due to its parallel processing capability, the throughput remains at a high level.

**(2) Delay experiment results**

This article sets up 20 nodes to participate in consensus, and Figure 3 shows different consensus algorithms

The delay obtained as the number of consensus changes. From Figure 3, it can be seen that as consensus increases.

As the number increases, the consensus delay gradually increases. The consensus algorithm for pure credit has a delay,The lowest is followed by credit+BFT, followed by credit+other consensus mechanisms, and finally

Credit+PoX class. In pure credit consensus algorithms, the consensus of CCAC algorithm

The latency is lower than that of the SCACS algorithm. The main reason is that the latter

selects based on credit space.Miners have added a layered penalty mechanism, resulting in greater latency. Credit+its.

Compared with the credit+BFT class, his consensus algorithm has a larger latency, which is due to the ECCA

We adopted a trust propagation model to evaluate the node's credit rating, which is higher than BFT in terms of time， Class. Among the algorithms of Credit+PoX, CPoW has the highest consensus latency,

CPoS comes second. CPoW solves the hash problem as the length of the blockchain increases

The difficulty of consensus will also increase exponentially, which will consume a lot of computing power and result in higher consensus latency.And CPoS is based on using node voting to elect miner nodes, avoiding complexity,Hash operation for. The delay of CABP compared to ReCon in credit+BFT algorithms,Higher, because the former refers to neural network models to calculate the credit value of nodes,Compared to linear calculation methods, it is more time-consuming.

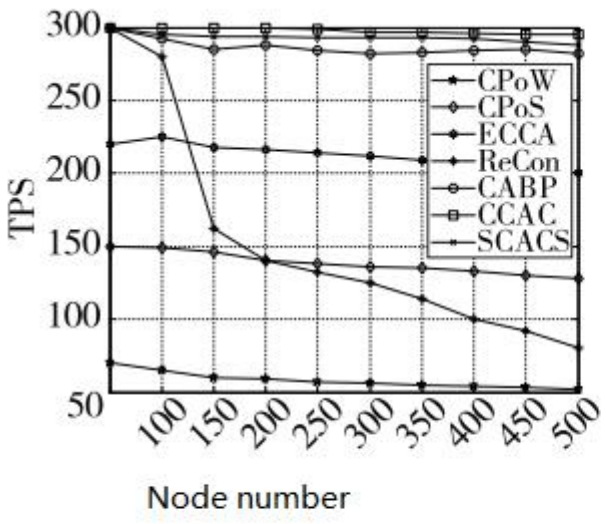


Fig. 2 Experimental results of throughput

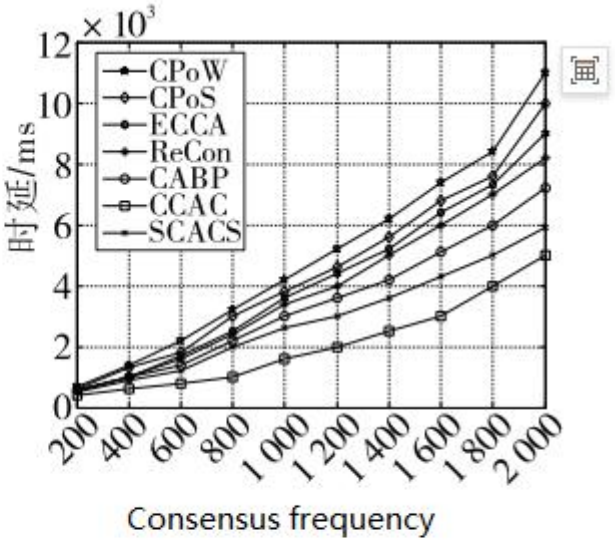


Fig. 3 Experimental results of delay

**(3) Experimental results of decentralization degree**

This article sets up 20 nodes to participate in consensus and assigns 1-20 numbers to the

nodes,Conduct 600 consensus sessions and count the number of times odd numbered nodes become miners,The results are shown in Figures 4 and 5. Due to the use of committees in reference [17] instead of a single one，Because of the miner node, only the other six consensus algorithms were compared. Divide by probability，If 20 nodes are equally likely to become mining nodes, then each node becomes a mining nodeThe probability of working is 1/20 × 100%=5%. In Figure 4, there are four types of credit+existing totalThe comparison results of the recognition mechanism show that the CPoW algorithm has a total of 8 nodes as shown in the figure，The probability is between 0% and 10%, ECCA is 7, while CPoS and CABP are both 6，However, the last three algorithms have more nodes that are 5% away from the baseline. Deserve.Note that the highest probability for CPoS, ECCA, and CABP nodes is 15%,ECCA appears three times, CABP twice, and CPoS once, which means ECCA is easier to perform

An oligopoly node appears. From Figure 4, it can be concluded that among the four algorithms, CPoW has

The degree of decentralization is better, followed by CPoS and ECCA. The reason is that

CPoW allows all nodes to participate in consensus, although nodes with high credit values will receive more

The search space is limited, so the probability of solving the hash problem is higher, but it does not mean that

Nodes with low credit values cannot be solved earlier. CPoS, ECCA, and

CABP selects miners from nodes with credit values above the threshold, not all

All nodes have a chance to be selected, and ECCA is the node with the highest credit rating

Centralized and random selection of leader nodes makes it easier to form a credit oligopoly.

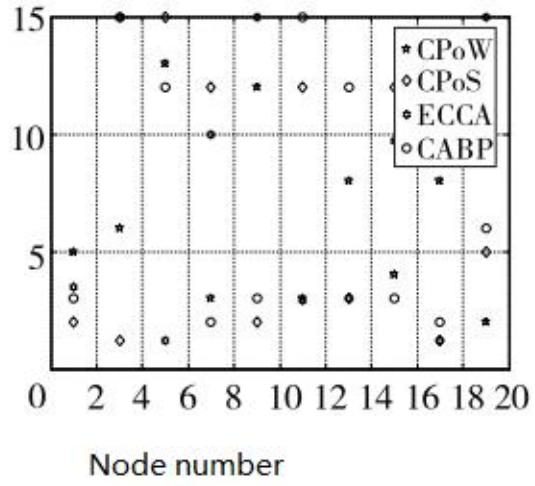


Fig. 4 Experimental results of decentralization 1

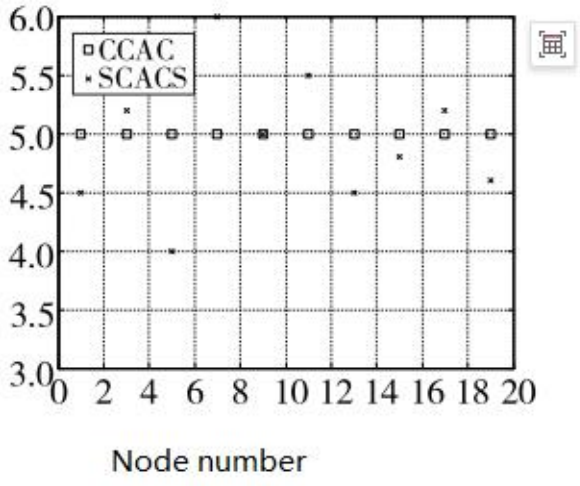


Fig. 5 Experimental results of decentralization 2

Fig. 5 shows the comparison results of two pure credit consensus methods. From the graph, it can be seen that

Each CCAC node has an equal probability of becoming a miner node, which is related to the implementation of the algorithm

The principle is directly related, and each cycle in CCAC selects credit values in descending order in sequence

The nodes in the sequence become miners, with the highest degree of decentralization. The variation pattern of SCACS.It oscillates around 5%, with a lower degree of decentralization compared to CCAC, but this does not

Certainty increases the safety of selecting miner nodes. SCACS enables each node to

The main reason for the consistent probability of becoming a miner is that the threshold mechanism can effectively suppress，The emergence of "oligopoly" nodes, the more times a node becomes a miner, the more

The credit value is increasing slowly and requires longer consensus time.

(4) Experimental results on the probability of malicious node eviction

Starting from the 5th round of consensus, this article sets 20% of the 20 nodes as

The experimental results of the expulsion probability of malicious nodes are shown in Figure 6. From Figure 6

Currently, most credit consensus algorithms use credit values to select Miner's Day

Point, lacking integration with other steps in consensus algorithms. In fact, block validation.

Synchronization is also a key factor affecting consensus efficiency. Due to the existing blockchain links.

The communication method of points is basically P2P, and the time complexity of communication is usually.O (n2). Structured communication topologies can be used to reduce communication complexity, Ji As early as 2012, et al. [34] proposed the use of a tree topology structure in consensus algorithms, which

The master node serves as the root node, and synchronous messages are traversed through a tree graph from the root node

The time complexity of line transmission and communication can be reduced to O (nlog2n), but it cannot be guaranteed

The main node is not a Byzantine node. Du et al. [35] proposed to divide synchronous nodes into main ones

Active and passive nodes, where the active node sends messages to the passive node using a tree structure

Transmission, this method significantly reduces the time complexity of communication, but there is also active.The risk of node misconduct causing serious hidden dangers to the system.In order to fully utilize the advantages of tree structure in communication complexity and effectively solve.To determine the impact of malicious nodes on system performance, the credit value of the node can be used to construct models such as

The tree communication topology shown in Figure 7. Sort nodes by credit value and number them

The node with a value of 1 has the highest credit value, which means that the node with a high credit value is in the.

The higher layers and parent nodes of a tree communication topology are more likely to have lower credit values, with nodes with lower credit values being at the bottom

Layer or leaf node. Usually, nodes with low credit values have a high probability of success,Evil, due to being at the bottom of a tree structure or even leaf nodes, even if it is harmful to ,The impact on the entire system can be limited to a lower range by designing appropriate nodes

Replacement strategy can ensure the normal operation of system communication

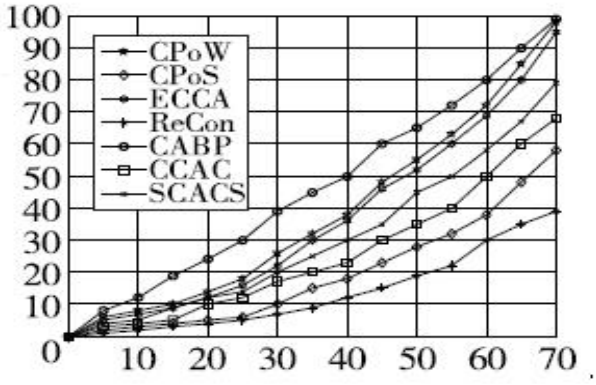


Fig. 6 Experimental results of malicious node eviction

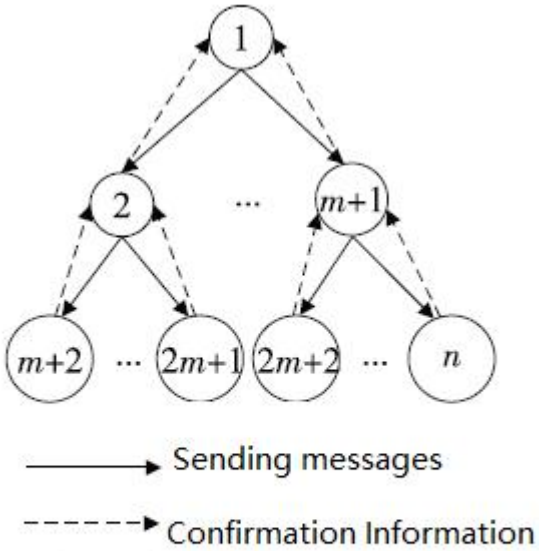


Fig. 7 Tree communication topology

It can be seen that as the number of consensus attempts increases, the probability of malicious nodes being evicted increases

Reference from Issue 2 Liu Huiwen, et al.: Comparative Study of Credit Based Blockchain Consensus Algorithms Page 325

The performance of CABP and CPoW methods is leading the other methods in terms of performance, as they continue to grow。 When the consensus round reaches 70 rounds, basically all malicious nodes can be expelled. Primary。Because both methods used neural network methods to evaluate node credit,

Can more accurately detect malicious node behavior. ECCA has built a relatively complete message

Using a rating evaluation model, once a malicious node appears, its credit rating will decrease, becoming

The probability of mining nodes is almost zero, and malicious nodes will be removed when the consensus round reaches 50 times

The probability of point expulsion has reached 50%. CPoS, CCAC, and SCACS methods work together

When the recognition round reaches 65, the probability of evicting malicious nodes

reaches 50%, while ReCon

The method has the worst ability to expel malicious nodes because ReCon does not use a single。

If a node serves as a miner node and instead adopts the method of collective bookkeeping by the committee, then

It is difficult to detect the wrongdoing of a single node because as long as consensus is reached, even if a node engages in wrongdoing， Evil, malicious nodes will also receive rewards from it.

## Conclusion:

By analyzing the highest proportion of collusion computing power in sub chains with different granularity and malicious node ratios, it can be concluded that overall, the AANS algorithm has a relatively low proportion of collusion computing power and a lower risk of collusion attacks. However, the proportion of malicious node collusion computing power only brings the risk of collusion attacks. In order to further analyze the security of AANS algorithm, it is necessary to compare the proportion of sub chain collusion attacks under different granularity of chain partitioning. Set the malicious node ratio to 40%, and set the chain granularity to 3, 5, 7, and 10.

From Figure 8, it can be seen that under different chain granularity, the proportion of sub chain collusion attacks in Zilliqa and Omniledger is greater than 0, and both sub chains are attacked by malicious nodes in collusion. Among them, the Zilliqa algorithm accounts for 40% of malicious nodes, and when the chain granularity is 3, the proportion of sub chain collusion attacks reaches 67%. At this time, the proportion of sub chain collusion attacks by malicious nodes is the highest. However, the AANS algorithm only experienced collusion attacks when the granularity of the chain was 10, and there was no collusion attack problem in other cases.

In summary, through the above experimental analysis, it can be concluded that the AANS algorithm can evenly allocate malicious nodes and their computing power to each sub chain, reducing the aggregation of malicious nodes in the sub chain, avoiding the fluctuation of the proportion of collusive computing power, and effectively reducing the risk caused by collusive attacks in the sub chain

In order to address the scalability issues of blockchain, this article constructs a

parallel multi chain performance optimization model from the perspective of modifying the underlying network architecture. This model improves the throughput of blockchain business processing and enhances the scalability of the system. On this basis, a network sharding algorithm (AANS) against collusion attacks is proposed to address the sub chain security issues in parallel multi chain blockchain models. This algorithm polls all malicious nodes in the blockchain network, evenly allocating malicious nodes and their computing power to each sub chain, preventing malicious nodes from occupying a large number of sub chains, resulting in 51% attacks caused by malicious node computing power aggregation. The experimental results show that under different granularity of fragmentation, the sub chain collusion computational power and sub chain collusion attack proportion of AANS algorithm are lower than existing network fragmentation algorithms, which to some extent improves the security of parallel multi chain models. When designing the network sharding algorithm in this article, the trust threshold was used to determine whether a node is a malicious node. The evaluation criteria for node behavior characteristics were not specifically studied. Therefore, how to design a reasonable node behavior feature determination scheme to make the identification of malicious nodes more accurate is the direction of future research。

**Acknowledgements：**

I want to thank my family and friends for their selfless support, encouragement, and research support. During this period, they provided me with unwavering support and understanding, encouraging me to continue pursuing knowledge and breakthroughs.

Without their support and understanding, I would not be able to complete this paper.Thank you to the professors of Odessa State University in Ukraine, Professor Eugene V. Malakhov and Professor Oleksandr Antonenko.

## REFERENCES

[1] HE JI, “Optimizing data security and stability of blockchain technology in the global value exchange system” International Journal of Science,Volume 10 Issue 8,http://www.ijscience.org ISSN: 1813-4890, 2023 IJS-ijscience.org-10-8-25-32

[2] BouragaS. Ataxonomyofblockchainconsensusprotocols: asurvey andclassificationframework[J]. ExpertSystemswithApplications, 2021, 168: 114384.

[3] AmaniA, SunF, RichardRB, etal. Availabilit

yanalysisofapermissionedblockchainwithalightweightconsensusprotocol[J]. Computers&Security, 2021, 102: 102098.
[4] SallalM, OwensonG, SalmanD, etal. Security andperformanceevaluationofmasternodeprotocolbasedreputationblockchaininthebitcoinnetwork[J]. Blockchain: ResearchandApplications, 2022, 3(1): 49 64.
[5] LiuYuan, LanYixiao, LiBoyang, etal. Proofoflearning(PoLe): empoweringneuralnetworktrainingwithconsensusbuildingonblockchains[J]. ComputerNetworks, 2021, 201: 108594.
[6] FerdousMS, ChowdhuryMJM, HoqueMA. Asurveyofconsensus algorithmsinpublicblockchainsystemsforcrypt currencies[J]. JournalofNetworkandComputerApplications, 2021, 182: 103035.
[7] LiuJun, XieMingyue, ChenShuyu, etal. AnimprovedDPoSconsensusmechanisminblockchainbasedonPLTSforthesmartautonomous
·326· Computer Application Research Volume 40
multi robotsystem[J]. InformationSciences, 2021, 575: 528 541.
[8] FanYuqi, WuHuanyu, PaikHY. DR BFT: aconsensusalgorithm forblockchain basedmulti layerdataintegrityframeworkindynamic edgecomputingsystem[J]. FutureGenerationComputerSystems, 2021, 124: 33 38.
[9] Wang Zuan, Tian Youliang, Li Qiuxian, et al. Workload Proof Algorithm Based on Credit Model [J]Journal of Communications, 2018, 39(8): 185 198.(WangZuan, TianYouliang, Li Qiuxian, etal. Proofofworkalgorithm basedoncreditmodel[J]. JournalonCommunications, 2018, 39(8): 185 198.)
[10] Wang Ruijin, Guo Shangtong, Qiu Weihong, et al. Master-slave multi chain layering based on credit voting consensus Cross chain model [J]. Journal of University of Electronic Science and Technology, 2021, 50(6): 907 914.
(WangRuijin, GuoShangtong, QiuWeihong, etal. A master slave multi chainhierarchicalcross chainmodelba

sedoncreditvotingcon
sensus[J]. JournalofUniversityofElectronicS cienceand
TechnologyofChina, 2021, 50(6): 907 914.)

[11]ZhuangQianwei, LiuYuan, ChenLisi, etal. Pr oofofreputation: a
reputation basedconsensusprotocolforblock chain based systems
[C]//ProcofBlockchainandInternetofThingsCo nference. New
York: ACMPress, 2019: 131 138.
[12]HuangJunqin,KongLinghe,ChenGuihai,etal.B IoT: blockchain
drivenInternetofThingswithcredit basedcon sensusmechanism
[C]//Procofthe39thIEEEInternationalConfere nceonDistributed
ComputingSystems. Piscataway, NJ: IEEEPress, 2 019: 1348 1357.
[13] Huang Jiacheng, Xu Xinhua, Wang Shichun. Improvement Plan for the Consensus Mechanism of Entrusted Equity Proof

[J]. Computer Applications, 2019, 39(7): 2162 2167.(Huang Jiacheng, Xu
Xinhua, WangShichun. Improvedschemeofdelegat edproofofstake
consensusmechanism[J]. JournalofComputerApp lications,
2019, 39(7): 2162 2167.)
[14] BugdayA, OzsoyA, ?ztanerSM, etal. Creating consensusgroup
usingonlinelearningbasedreputationinblock chainnetworks[J].
PervasiveandMobileComputing, 2019, 59(C): 101 056.
[15] LiFengqi, LiuKemeng, LiuJing, etal. DHBFT: dynamichierarchical
Byzantinefault tolerantconsensusmechanism basedoncredit[C]//
ProcofAsia PacificWeb (APWeb) and Web AgeIn formation
Management(WAIM) JointInternationalConferen ceonWebandBig
Data. Berlin: Springer, 2020: 3 17.
[16] OliveiraMTD, ReisLHA, MedeirosDSV, etal. B lockchainreputa
tion basedconsensus: ascalableandresilientm

echanismfordistributed mistrustingapplications[J]. ComputerNetworks, 2020, 179: 107367.
[17] BiryukovA, FeherD. ReCon: sybil resistant consensusfromreputation[J]. PervasiveandMobileComputing, 2020, 61: 101109.
[18] WangEK, LiangZuodong, ChenCM, etal. PoRX: a reputationincentiveschemeforblockchainconsensusofIIoT[J]. FutureGenerationComputerSystems, 2020, 102: 140 151.
[19] Liu Haozhe, Li Shasha, Lv Weilong, et al. Consensus on master-slave multi chain blockchain based on credibility Mechanism [J]. Journal of Nanjing University of Science and Technology, 2020, 44(3): 325 331.(LiuHaozhe, LiShasha, LyuWeilong, etal. Master slavemultiple blockchain consensusbasedoncredibility[J]. JournalofNanjingUniversity ofScienceandTechnology, 2020, 44(3): 325 331.)
[20] SunLijun, YangQian, ChenXiao, etal. RC chainreputation based crowdsourcingblockchainforvehicularnetworks[J]. JournalofNetworkandComputerApplications, 2021, 176: 102956.
[21] MershadK, CheikhrouhouO, IsmailL. Proofof accumulatedtrust: a newconsensusprotocolforthesecurityoftheIoV[J]. Vehicular Communications, 2021, 32: 100392.
[22] Li Shuzhi, Huang Lei, Deng Xiaohong, et al. Credit based alliance chain consensus algorithm [J]. Calculation Research on Computer Applications, 2021, 38(8): 2284 2287.(LiShuzhi, HuangLei, DengXiaohong, etal. Consortiumchainconsensus algorithmbasedon credit[J]. ApplicationResearchofComputers, 2021, 38(8): 2284 2287.)
[23] Zhou Yihua, Jia Liyuan, Jia Yuxin, et al. Hashgraph consensus algorithm based on reputation[J]. Research on Computer Applications, 2021, 38(9): 2590 2593.(ZhouYihua, JiaLiyuan, JiaYuxin, etal. Hashgraphconsensus algorithmbasedon credit[J]. ApplicationResearchofComputers, 2021, 38(9): 2590 2593.)
[24] MohsenzadehA, BidgolyAJ, FarjamiY. Afairc

onsensusmodelin
blockchainbasedoncomputationalreputation[J]. ExpertSystems
withApplications, 2022, 204: 117578.
[25] DengXiaohong, LiKangting, WangZhiqiang, etal. Anovelconsensus
algorithmbasedonsegmentedDAGandBPneuralnetworkforconsor
tium blockchain[J]. SecurityandCommunication Networks,
2022, 2022: articleID1060765.
[26] MohsenzadehA, BidgolyAJ, FarjamiY. Anovel reputation based
consensusframework(RCF) indistributedledger technology[J].
ComputerCommunications, 2022, 190(C): 126 144.
[27]DengXiaohong,LuoZhiqiong,ZouYijie,etal.Anovelsemifragile
consensusalgorithmbasedoncreditspaceforconsortiumblockchain
[J]. SecurityandCommunicationNetworks, 2022, 2022: article
ID1955141.
[28] Chen Yourong, Chen Hao, Han Meng, et al. Consensus on Medical Data Security Based on Credit Rating Classification Algorithm [J]. Journal of Electronics and Information Technology, 2022, 44(1): 279 287.(ChenYou
rong, ChenHao, HanMeng, etal. Securityconsensu salgorithm of
medicaldatabasedoncreditrating[J]. JournalofElectronics&
InformationTechnology, 2022, 44(1): 279 287.)
[29] Chen Yourong, Zhang Yang, Chen Hao, et al. Efficient and Consistent Blockchain for Heterogeneous Nodes in the Internet of Vehicles
Research on Sexual Consensus Algorithms [J]. Journal of Electronics and Information Technology, 2022, 44(1): 314 323.
(ChenYourong, ZhangYang, ChenHao, etal. Efficient consistency
consensusalgorithmofblockchainforheterogeneousnodesintheIn
ternetofVehicles[J]. JournalofElectronics&InformationTech
nology, 2022, 44(1): 314 323.)
[30]Huang Baohua, Qu Xi, Zheng Huiying, et al. A credit based Byzantine fault-tolerant consensus algorithm[J]. Information Network Security, 2022, 22(4): 86 92.(HuangBaohua, Qu
Xi, ZhengHuiying, etal. A credit basedByzanti nefaulttolerance
consensusalgorithm[J]. NetinfoSecurity, 2022,

22(4): 86 92.)
[31] AlhasnawiBN, JasimBH, SedhomBE, etal. Consensusalgorithm basedcoalitiongametheoryfordemandmanagementschemeinsmart microgrid[J]. SustainableCitiesandSociety, 2021, 74: 103248.
[32] Ren Nan, Ma Yuanyuan. Evolutionary Game and Strategy Research on Improving DPoS Consensus Mechanism [J] Computer Engineering and Applications, 2022, 58(12): 102 111.(RenNan, Ma Yuanyuan. Researchonevolutionarygameandstrategyof DPoSconsensusmechanism improvement[J]. ComputerEngineeringand Applications, 2022, 58(12): 102 111.)
[33] Yang Xinyu, Peng Changgen, Yang Hui, et al. A Rational Byzantine Fault Tolerant Consensus Based on Evolutionary Games Algorithm [J]. Computer Science, 2022, 49(3): 360 370.(YangXinyu, Peng Changgen, YangHui, etal. RationalPBFTconsensus algorithm with evolutionarygame[J]. ComputerScience, 2022, 49(3): 360 370.)
[34] JiZhijian, LinHai, YuHaisheng. Leadersinmulti agentcontrol labilityunderconsensusalgorithmandtreetopology[J]. Systems& ControlLetters, 2012, 61(9): 918 925.
[35] DuLiang, TaoYuan, ChenTianmei, etal. AnadvancedPBFT based consensusalgorithmforabiddingconsortiumblockchain[C]//Proc ofthe3rdInternationalConferenceonBlockchainTechnology. 2021: 176 182.
[36] Gao Zhengfeng, Zheng Jilai, Tang Shuyang, et al. Distributed ledger consensus mechanism based on DAG Research [J]. Journal of Software Science, 2020, 31(4): 1124 1142.(GaoZhengfeng, ZhengJilai, TangSuyang, etal. State of the art surveyofconsensus mechanismsonDAG baseddistributedledger[J]. JournalofSoftware, 2020, 31(4): 1124 1142.)
[37] FuXiang, WangHuaimin, ShiPeichang, etal. Teegraph: ablock chainconsensusalgorithmbasedonTEEandDAGfordatasharingin IoT[J]. JournalofSystemsArchitecture, 2022, 122: 102344.

[38]WangShangping,LiHuan,ChenJuanjuan,etal.DAGblockchain
basedlightweightauthenticationandauthorizationschemeforIoTde
vices[J].JournalofInformationSecurityandApplications,
2022,66:103134.

[39] Xia Qing, Dou Wensheng, Guo Kaiwen, et al. Overview of Blockchain Consensus Protocol [J]. Journal of Software
2021,32(2):277 299.(XiaQing,DouWensheng,Guo Kaiwen, et
al.Surveyonblockchainconsensusprotocol[J].JournalofSoft
ware,2021,32(2):277 299.)