Computers, Materials & Continua
DOI: 10.32604/cmc.2022.028757
Article

Tech Science Press

A Dynamic Reputation–based Consensus Mechanism for Blockchain

Xiaofang Qiu[1,2], Zhi Qin[1,2,*], Wunan Wan[1,2], Jinquan Zhang[1,2], Jinliang Guo[1,2], Shibin Zhang[1,2] and Jinyue Xia[3]

[1]School of Cybersecurity, Chengdu University of Information Technology, Chengdu, 610225, China
[2]Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chengdu, 610225, China
[3]International Business Machines Corporation(IBM), NewYork, 10041NY212, USA
*Corresponding Author: Zhi Qin. Email: cuitqz@qq.com
Received: 16 February 2022; Accepted: 12 April 2022

Abstract: In recent years, Blockchain is gaining prominence as a hot topic in academic research. However, the consensus mechanism of blockchain has been criticized in terms of energy consumption and performance. Although Proof-of-Authority (PoA) consensus mechanism, as a lightweight consensus mechanism, is more efficient than traditional Proof-of-Work (PoW) and Proof-of-Stake (PoS), it suffers from the problem of centralization. To this end, on account of analyzing the shortcomings of existing consensus mechanisms, this paper proposes a dynamic reputation-based consensus mechanism for blockchain. This scheme allows nodes with reputation value higher than a threshold apply to become a monitoring node, which can monitor the behavior of validators in case that validators with excessive power cause harm to the blockchain network. At the same time, the reputation evaluation algorithm is also introduced to select nodes with high reputation to become validators in the network, thus increasing the cost of malicious behavior. In each consensus cycle, validators and monitoring nodes are dynamically updated according to the reputation value. Through security analysis, it is demonstrated that the scheme can resist the attacks of malicious nodes in the blockchain network. By simulation experiments and analysis of the scheme, the result verifies that the mechanism can effectively improve the fault tolerance of the consensus mechanism, reduce the time of consensus to guarantee the security of the system.

Keywords: Blockchain; consensus mechanism; proof-of-authority; reputation evaluation

1 Introduction

Bitcoin has been born since Satoshi Nakamoto published his famous paper "Bitcoin: A Peer-to-Peer Electronic Cash System" [1] in November 2008. With the development of Bitcoin, blockchain as the underlying technology of Bitcoin has officially come into the spotlight. Blockchain is essentially

a multi-participant, jointly maintained, and continuously growing distributed database using cryptographic technology. Each block is interconnected by saving the hash value of the previous block, forming a chain structure with features such as decentralization, anonymity, and immutability. Based on these features, blockchain is gradually been widely used in recent years in the fields of digital currency, finance [2], Internet of Things [3,4], and healthcare [5,6].

The core technologies of blockchain include cryptographic principles, consensus mechanisms, and smart contracts, each of which plays its own important role in the blockchain network. In a blockchain network, all nodes can generate transactions by broadcasting messages, and the miner nodes in the network verify and package a set of transactions to form a block. The miner node that successfully generates a block can broadcast the block to the network, and when all other nodes add this block to the local blockchain they maintain, it means that there is a consensus on the generation of this block. However, due to the unreliability of nodes and the instability of communication between nodes, or even malicious nodes forging information for malicious response, there is the problem of inconsistent data state between nodes. How to make each node reach consensus on the validity and consistency of transactions in a distrustful decentralized system has been the problem of blockchain technology research.

Consensus mechanism is one of the most important components of blockchain technology, which is the key to form multiple unreliable individual nodes into a reliable distributed system, and mainly addresses how to achieve consistency of blockchain in distributed scenarios. Consensus mechanism plays a crucial role in maintaining the security and efficiency of blockchain, and using the right consensus mechanism can enhance the system performance and promote the widespread application of blockchain technology. So far, there are many different types of blockchain consensus mechanisms.

The main consensus mechanisms in the current blockchain network are PoW, PoS, Practical Byzantine Fault Tolerance (PBFT) and other improved consensus mechanisms based on these. These different consensus mechanisms solve different problems. In different application scenarios, we should choose the most appropriate consensus mechanism.

In this paper we analyze the advantages and shortcomings of the PoA mechanism and propose a dynamic reputation-based consensus mechanism for the permission Chain. Firstly, the validators and monitoring nodes are selected at the beginning of the consensus, and the validators perform block packing by pledging its own reputation value, and the monitoring nodes monitor the behavior of the validators. Then a new reputation evaluation algorithm is proposed based on the historical reputation of nodes and the behavior of nodes participating in the current consensus process, which is used to dynamically update the reputation value of each mode. Finally, all of validators and monitoring nodes are replaced according to their reputation value. The security analysis and experimental simulation of this scheme are carried out.

The rest of the paper is organized as follows. We discuss related work in Section 2. Section 3 introduces the dynamic reputation-based consensus mechanism. Section 4 presents the security analysis. Section 5 conducts simulation experiments on this consensus mechanism and analyzes the experimental results. Section 6 concludes the paper.

2 Related works

2.1 Consensus Mechanism

The core of the blockchain is the consensus mechanism, but the consensus mechanism was studied much earlier than the blockchain. Akkoyunlu and Ekanadham proposed the "Two Generals'

Problem" in the computers field in 1975 [7], which revealed that it is difficult to achieve consistent communication when the transmission channel is unreliable and there are no defectors. The key of the two generals' problem is that the channel is unreliable. In reverse, two generals' problem is solvable in a reliable channel. But there is no reliable channel, so it is unsolvable in the classic situation. In 1982, Leslie Lamport and two other people proposed "The Byzantine Generals Problem" [8], which assumes that the channel is reliable but there may be faulty nodes, and investigates how non-faulty nodes can reach consistency under this premise. Since then, distributed consensus has been divided into Byzantine fault-tolerant consensus and non-Byzantine fault-tolerant consensus. The Byzantine Generals problem is the root of the core idea of blockchain technology, which directly affects the design and implementation of consensus mechanism for blockchain systems.

PoW is the first blockchain consensus mechanism to ensure the consistency of Bitcoin network database. the core of PoW is that miners compete with their own computing power to solve a mathematical problem, and the node who solves the problem first obtains the right of accounting ledger. The advantage of PoW is that it has a high degree of decentralization. As the computing power of the entire network increases, the cost of an attack also increases. However, the large amount of energy consumption required to generate block and the long transaction time are significant shortcomings of PoW. In 2012, Sunny implemented the PoS mechanism in PPcoin [9], PoS obtains the right of accounting ledger by pledging token instead of computing power. PoS effectively solves the energy consumption problem of PoW, while shortening the consensus time and improving the transaction speed and throughput. However, because mining does not require cost, PoS forks will be more common than PoW, and are more likely to be attacked by double spending. But the low degree of decentralization will lead to the problem of token monopoly. PoS and PoW mechanisms focus on competition for the right of accounting ledger and are suitable for public networks. Our mechanism focuses on blockchain applications based on permission chains, in which consensus can be reached without competition.

PoA is a new Byzantine family consensus mechanism that restricts block generation to a fixed set of nodes. The core of PoA is to designate a fixed validator or a set of validators who verify and package the transactions in the network, then other nodes directly copy data from the validators. Therefore, the PoA mechanism does not require competition for the right of accounting ledger, and the security of the blockchain is guaranteed by the validators. So PoA has a high degree of scalability. It is often considered as a compromise between a true decentralization and an efficient centralized system. Retail giant Walmart has incorporated MediLedger into its tracking system to improve the efficiency of supply chain management. The MediLedger project uses the enterprise version of the Ethereum to track the origin of medicines through the PoA consensus mechanism. Unlike the PoW mechanism, PoA is not resource-intensive. It is lightweight and has higher throughput. Therefore, it is an ideal consensus mechanism for localized IoT blockchain implementations. In the case of smart homes that power consumption is key, there is a limit to the computational and storage capacity of the device. In [10], the authors use PoA consensus mechanism to manage the devices in smart homes and the experiment demonstrate that the system using POA consensus mechanism consumes less energy and is more efficient. In [11], the authors investigate the applicability of blockchain technology in smart grid, and discuss different solutions and highlight the adaptability of PoA consumes in smart grid scenarios. In [12], a permission blockchain with PoA technology is proposed, which can guarantee data privacy, control of data owners over sharing their sensitive information, and efficient distributed management of healthcare records. In [13], the authors propose a blockchain system based on improved PoA consensus, and this scheme uses hash algorithms, smart contracts to solve the problem of occupying seats in the field of civil aviation.

However, if the validator in the PoA mechanism does evil by himself and launches an attack on the network or tampers with the ledger, it is easy to cause harm to the entire blockchain network. This paper introduces a dynamic reputation model in the POA mechanism to solve the security problem of validator.

2.2 Reputation-based Trust Model

Trust models first started with Marsh's introducing trust relationships in social relationship networks into computer networks. Later researchers established various trust models based on different mathematical methods and tools to describe trust dynamics and system uncertainty. The typical trust models in distributed systems mainly include Eigen Trust model [14] and Peer Trust model [15], which are used for trust evaluation of distributed network nodes to avoid untrusted transaction objects and improve the security of transactions. The Eigen Trust model is a global trust model. On this model, the direct trust values among nodes iteratively calculates the global trust value, and the recommendation behavior of nodes with high trust is proposed to be reliable. The Peer Trust model is similar to the Eigen Trust in the principle of constructing trust based on recommendations, both of which are based on mutual recommendations among nodes for global trust evaluation. However, the Peer Trust model calculates the direct reputation of a node based on the interaction evaluation among nodes, and the feedback evaluation among nodes, the number of transactions, the trustworthiness of the feedback evaluation, the transaction time, the amount and the environment are used as calculation factors to calculate the reputation value of a node. In the PoA consensus, only a portion of nodes are allowed to act as validators. So once these validators are dishonest, then the consensus mechanism will also be damaged. Therefore, adding a trust evaluation mechanism is necessary. In the literature [16], a trust model is added to PBFT consensus to evaluate the behavior of each node, add a dynamic incentive mechanism to select nodes with high trust as master nodes, and reduce the participation of malicious behavior in consensus. In [17], the trust model is introduced to solve the bribery problem in the proof-of-stake mechanism and the selfish mining problem in the proof-of-work. In the literature [18], it is defined that the credit of a node only depends on the behavior of the node, and the node obtains the accounting right through credit verification. Literature [19] propose a Blockchain reputation-based consensus, which randomly selected a set of judge nodes monitor the nodes in the consensus process. Only nodes with credit values higher than the trust threshold can obtain the accounting right. However, the selection of miner nodes is only based on the maturity criterion. The judge nodes and miner nodes will not change once they are matched. Therefore, this paper proposes a dynamic reputation-based blockchain consensus mechanism that evaluates the reputation of nodes based on their behavior, raises the threshold to become a validator. The blockchain network is maintained by monitoring nodes to monitor the behavior of the verifying nodes in order to avoid the harm to the blockchain network caused by the excessive power of the validator in the POA mechanism.

3 Dynamic Reputation-based Consensus Mechanism

The dynamic reputation-based consensus mechanism proposed in this paper mainly includes the monitoring nodes group generation algorithm, the validators group generation algorithm, node behavior discrimination and reputation evaluation algorithm. In PoA consensus, the blockchain selects a fixed set of validators to unify the state of the entire network, but the validators may not be completely trusted. Therefore, this scheme assigns a reputation value to each node through a reputation evaluation model. Each validator performs block packing by pledging its own reputation value, and all nodes can complete the reputation accumulation by maintaining the block chain. The trustworthiness of the validators is ensured by selecting the nodes with high reputation values to become the validator group.

3.1 Consensus Process

The consensus is divided into several cycles, and each cycle consists of a number of rounds. the mining process of this mechanism follows the order of higher to lower reputation of the validators in turn, with each round being mined by one validator. Step (1)-Step (5) show the specific process in each consensus cycle.

1. In the first consensus cycle, the initial monitoring nodes group is generated according to the monitoring nodes group generation algorithm and the initial validators group is selected according to the initial validators group generation algorithm.
2. The validator with the highest reputation value in the validators group verifies and packs a new block and broadcasts it to the monitoring nodes group. If the validator does not finish packing the block within the specified time, the next validator will start packaging in order.
3. After the validator verifies and packs the block. The monitoring node determines the behavior of the validator by verifying the correctness of the block, and if the validator completes the consensus behavior normally then token is awarded. If the validator consensus is abnormal then the monitoring node applies for the current round consensus invalidation and then jumping to next consensus round, consensus abnormalities include consensus timeout and the validator packaged wrong transactions in that round.
4. When the validators group all complete block packing, all nodes perform reputation evaluation based on the behavior of the consensus process in this cycle, and dynamically update the reputation value.
5. The next round of monitoring nodes group is generated according to the monitoring nodes group generation algorithm, and the next round of validators group is generated according to the next round of validators group generation algorithm. The current consensus cycle ends and enters the next consensus cycle. Fig. 1 illustrates the flow of a consensus cycle.

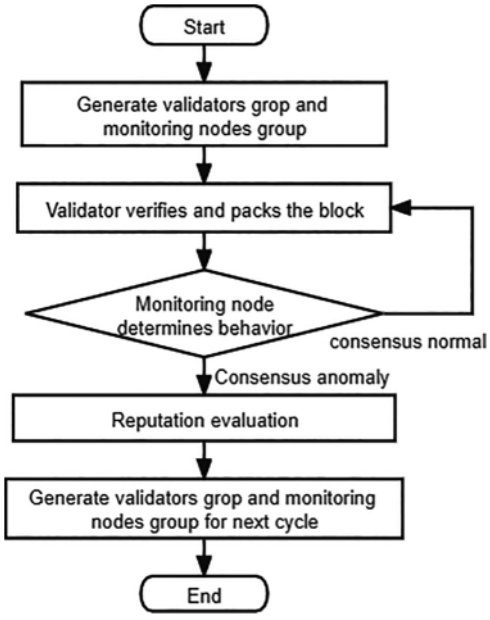

Figure 1: The flow of a consensus cycle

3.2 Monitoring Nodes Group Generation Algorithm

A monitoring nodes group is a set of monitoring nodes that monitor the behavior of validators. If enough monitoring nodes verify that the block is correct and signed, then the validator is judged to be "good" and is rewarded with a corresponding token. All signed monitoring nodes are then considered to have maintained the blockchain network. To prevent attackers from maliciously manipulating a group of nodes to sway the behavior of a validator, the initial reputation of a node is set to RT when it joins the network, and the monitoring node must have sufficient reputation (Re>=RT) to maintain the blockchain network.

Monitoring nodes group generation algorithm: Before the validators group is generated. All nodes with reputation higher than RT can apply to join the monitoring nodes group in a fixed time T1. If a monitoring node is elected as a validator in the validators group generation algorithm, it will automatically drop out of the monitoring nodes group. The monitoring of the behavior of the validator by the monitoring node is considered as the maintenance of the whole blockchain network. In this algorithm, the monitoring node is selected before the validator generated, so there is no manipulation of the monitoring node's selection by the validator, which ensures the fairness of the monitoring nodes group.

3.3 Validators Group Generation Algorithm

The relatively fixed validators group can cause problems such as transaction tampering and node' s credibility degradation. The validators group generation algorithm proposed in this paper is a dynamic validators group based on reputation. The members of the validators group change dynamically with time. In order to avoid overburdening the validator and thus leading to network inefficiency, the number of validators must grow in proportion to the number of active nodes in the blockchain network, and when the number of nodes joined in the network increases, the corresponding number of validators also increases.

Initial validators group generation algorithm: At the first consensus cycle, randomly select n% of the nodes that have just joined the network as the initial validators group.

Next round of validators group generation algorithm: After each cycle of the consensus process, each node has a reputation evaluation. Each node is given a reputation value, and the reputation values are sorted from high to low, and the top n% of nodes with high reputation values are selected to enter the validators group in the next cycle. After the node is selected as the validator in the next cycle, and sent their public key and other information to the blockchain network. Enter a new consensus cycle, and the new validators verify the transaction in the new cycle and generate new block.

3.4 Node Behavior Discrimination

Traditional consensus mechanisms rely solely on raising the entry threshold, such as computing power or stake, to maintain the stability and security of blockchain networks, but both of them tend to make blockchain networks centralized. In this paper, we propose a judgement strategy for the validators by verifying and judging of monitoring nodes in order to identify malicious nodes. Fig. 2 shows a consensus round where the monitoring nodes are monitoring the block which packed by validator.

In this paper, the consensus behavior validator is defined as "good" and "bad".

Good: After the validator generates a block, the monitoring node will verify the transaction and hash value in the block. If the block is correct, then the consensus behavior of corresponding validator

is defined as "good" and signed, and the block is confirmed in the blockchain network after multiple monitoring nodes sign it. The monitoring node that signed the block is considered to have completed a "good" consensus and the validator that generates a block is rewarded with tokens. The reputation of this scheme is used as the source of authority for the validators, and validators complete block packing by consuming a portion of their reputation, while the token incentive is the main source of incentive.

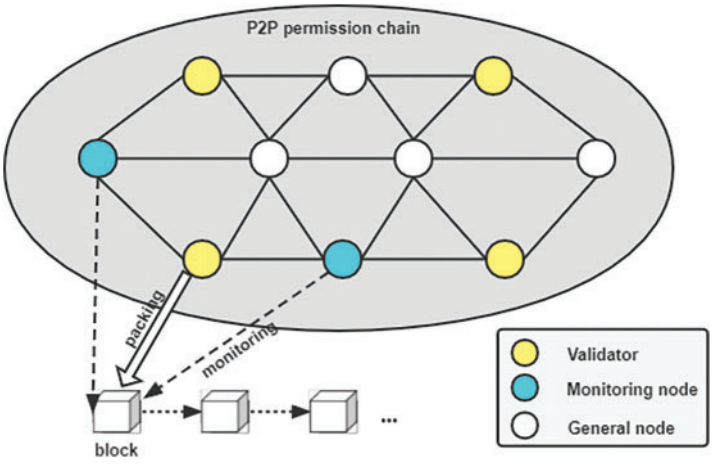

Figure 2: Monitoring nodes are monitoring the block

Bad: If a monitoring node finds a problem with the block it wants to verify, it defines the consensus behavior of corresponding validators as "bad". If it still wants to sign the block, then the other monitoring nodes in the monitoring nodes group will also verify the block. If the block contains a signature that is illegal or the block header hash is incorrect, then the block is considered illegal. All monitoring nodes that sign the block are considered to be bad and are penalized with a reputation punishment. The block is considered illegal. All monitoring nodes that perform signature operations on the block are considered to have performed a "bad" consensus behavior.

3.5 Reputation Evaluation

Because not all nodes in P2P networks are honest nodes, some nodes participate in consensus actively; some nodes are bad and feed false transaction information, causing consensus anomalies. Based on the research related to the trust model and combined with the PoA consensus mechanism, this paper proposes a new reputation evaluation algorithm which take the historical reputation of nodes and the behavior of nodes participating in the consensus process at this stage into account. This model is able to dynamically update the reputation of nodes, reduce the impact of erroneous nodes on the consensus process, and improve the fault tolerance and stability of the system. The reputation evaluation formula of node u is:

$$\mathrm{Re}_u^t = \alpha^* RH_u + \beta^* RC_u^t + \gamma^* RT_u^t \tag{1}$$

where Re_u^t denotes the reputation value of node u in cycle t and consists of three parts. Where RH_u is the historical reputation evaluation of node u, which is the reputation value inherited from the previous t consensus cycles of node u. RC_u^t is the consensus reputation evaluation of node u, which obtained from the consensus behavior of nodes in cycle t. RT_u^t is the transaction reputation evaluation of node u, which obtained from participation in transactions of node u in that consensus cycle. α, β, γ are the weights of these three components.

The consensus behavior of a node at present stage may be a continuation of the historical consensus situation. If a node makes honest behavior for a long time, we can guess that it has a high probability of continuing honest behavior then. The historical reputation evaluation of a node can reflect the reputation status of node. Therefore, we calculate the node's reputation value from previous cycles to get a historical reputation evaluation. The formula for calculating the historical reputation evaluation as follows:

$$RH_u = \sum_{k=1}^{t-1} \frac{\rho^{t-k} * \mathrm{Re}_u^k}{t-k} \tag{2}$$

where ρ denotes a time decay factor indicating the degree of influence of the reputation value of cycle k on the historical reputation evaluation. It is very high that the degree of influence of the node's reputation value in the previous cycle on its historical reputation evaluation. In the first consensus cycle, the value of ρ^{t-k} is very small. It indicates that the farther consensus cycle is from the current cycle, the greater the time decay and the smaller the influence on the node's historical reputation evaluation, it means the recent reputation value is more important. Node's frequent recent honest behavior led to higher reputation value, and more obvious promotion to its existing reputation evaluation.

The consensus reputation evaluation of nodes is obtained based on the consensus behavior of nodes during the request cycle, mainly for validators and monitoring nodes. The consensus reputation evaluation is calculated as follows:

$$RC_u^t = \frac{N_{good} - \lambda * N_{bad}}{N_{total}} \tag{3}$$

where N_{good} denotes the number of the node's consensus behavior is judged as "good". N_{bad} denotes the number of the node's consensus behavior is judged as "bad", and the λ is its weight. N_{total} denotes the total number of node consensus behaviors. RC_u^t increases as N_{good} increases, it means that the more times the node is judged as "good", the greater the positive impact on the consensus reputation evaluation. In order to prevent nodes from reducing the impact of "bad" behaviors by a large number of "good" behaviors, we set λ to increase the weight of "bad" behaviors,increasing the cost of malicious behavior.

The transaction reputation evaluation of a node is obtained based on the evaluations of other nodes with which the node generated transactions during the request cycle. The feedback evaluation among nodes, the number of transactions, and the credibility of the feedback evaluation are used as calculation factors to calculate the value of transaction reputation evaluation of a node. The transaction reputation evaluation is calculated as follows:

$$RT_u^t = \frac{\sum_{i=1}^{I(u)} S(u,i) * Cr(p(u,i))}{I(u)} \tag{4}$$

where $I(u)$ denotes the number of all transactions of node u. $S(u,i)$ denotes the feedback evaluation of the i_{th} transaction of node u by other nodes. $P(u,i)$ denotes the transaction object of the i_{th}transaction. $Cr(u)$ denotes the trustworthiness of the node. In general, the evaluation of nodes with high reputation value is more credible. As the reputation value of the evaluation node is higher, the value of $Cr(u)$ increases, the node's transaction reputation evaluation is also higher.

With the reputation-based evaluation algorithm, the reputation of a node can be evaluated and updated based on the behavior of the node in each cycle. The more honest behaviors a node has in the previous cycle, the higher its reputation value is, and the easier it is to be elected as the validator for

the next cycle to receive token rewards. Dynamically changing reputation ensures that the validators selected in each cycle are trustworthy.

4 Security Analysis

4.1 Double Spending Attack

Let attacker initiate a transaction that will later be revoked by him.

In this scheme, we use the PoA consensus mechanism. Nodes do not need to compete for accounting rights. The validator verifies the transaction when the block is packed, and the monitoring node also verifies the block in that time. Once the block containing the transaction is confirmed in the network, all nodes copy the block in a locally maintained blockchain so that the attacker cannot then revoke the transaction.

4.2 Malicious Validator Attacks

Let attacker is a malicious node that is elected as a validator after reputation accumulation. When it packs a block, it packs invalid transactions into the block.

A node that is elected as a validator after accumulating reputation must have done a lot of honest behavior in the network, and the cost of his malicious behavior is much higher than the effort of accumulating reputation in the network. The validator should behave well to be rewarded with tokens rather than committing malicious acts to attack the network. Even if the validator packages invalid transactions in blocks, the blocks will be judged as invalid due to the timely verification by the monitoring nodes. The malicious behavior of the validator will only affect itself reputation value.

4.3 Malicious Monitoring Node Attacks

Let attacker is a monitoring node for a certain verification node, and signs the illegal block after the validator generates a block.

In this scheme, monitoring nodes group is a set of nodes. If a monitoring node finds a problem with the block it wants to verify, it defines the consensus behavior of corresponding validator as bad. If it still wants to sign the block, then the other monitoring nodes in the monitoring nodes group will also verify the block. If the block contains a signature that is illegal or the block header hash is incorrect, then the block is considered illegal. All monitoring nodes that sign the block are considered to be bad and are penalized with a reputation punishment. The block is considered illegal. All monitoring nodes that perform signature operations on the block are considered to have performed a "bad" consensus behavior. This behavior will affect the consensus reputation evaluation of that node.

5 Experiments and Analysis

In order to test the results of this scheme, the experimental environment of this paper is Windows 10 operating system, system memory is 16G, CPU is Intel Core-i5 processor, and hard disk size is 500G. The experiments are based on the simulation of this scheme process in Python, and the development language is Python3.6. Through experiments to test the block generation time of the consensus algorithm of this scheme and the analysis of the node's accounting rights, the efficiency of this scheme and the resistance of the nodes to malicious behaviors are verified.

5.1 Blockchain Block-Generate Time Analysis

This scheme sets a time threshold in the consensus process for preventing the failure of single validator. Ensures stable block-generate in the blockchain network even if there is a malicious node. The time that spent for each block-generate is recorded, with intervals of every 10 blocks in the first 100 blocks, and the statistics are shown in Fig. 3.

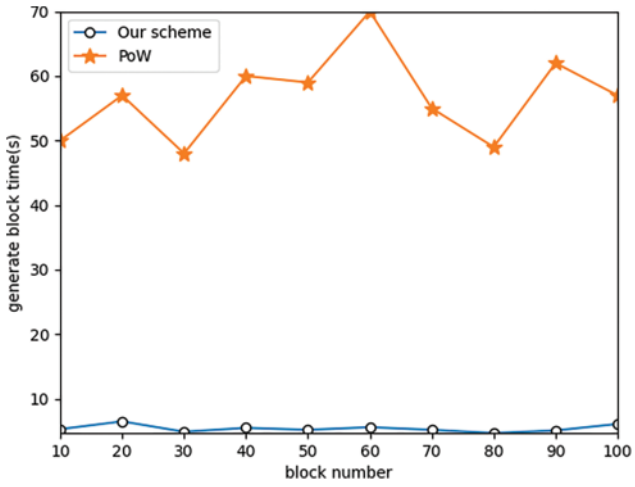

Figure 3: The time of block generation

The experimental results shows that the block-generate time of the consensus based on this scheme is very stable, and the vast majority of the block-generate time is around 5 s. Although a small part of the data fluctuates, the experimental results basically meet the requirements, which improves the transaction efficiency of the blockchain system and saves a lot of time.

5.2 Analysis of Node Accounting Times

The number of validators is n% of all nodes in order to reduce the burden of validators. The experiment sets n = 20, which means that when there are 10 nodes in the network, two validators are selected for each consensus cycle. We set node 1 actively participates in consensus and initiates transactions in the network. Set node 2 has frequent malicious behavior (invalid transactions or illegal consensus) in the network. Set node 4 participates in consensus normally but has shown malicious behavior. Node 5 neither participates in consensus behavior nor generates transactions rarely in the network. Set node 7 among these 10 nodes to participate in consensus less others in the network, but interact with other nodes actively. The rest of the nodes participate in consensus behavior normally. The number of these ten nodes are elected as validator in 100 consensus cycles is recorded, and the statistics are shown in Fig. 4.

The experimental results indicate that node 1 becomes validator most often because of its active and honest participation in various activities in the network. Node 2 becomes validator almost no times because of frequent malicious behaviors. Node 4 becomes validator less often than other honest nodes because of its malicious behavior. Node 5 becomes validator less often than other active nodes because of its low activity in the network. Node 7, although rarely involved in consensus behavior, has high activity in the network, so it becomes validator more often than node 5. The experimental results basically satisfy the requirements, weaken the centralization problem of the POA mechanism, and improve the security of the system.

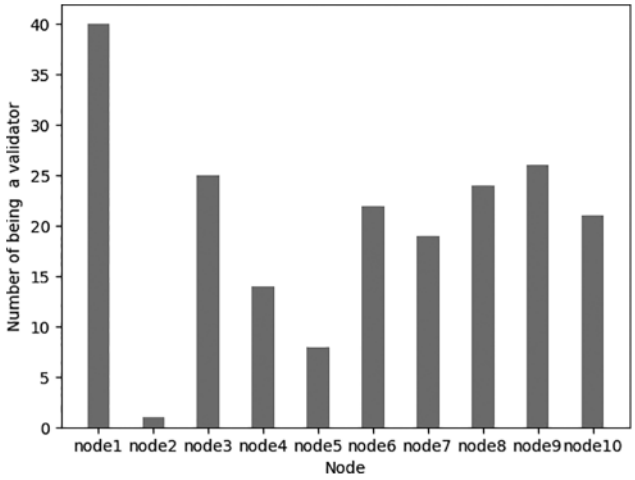

Figure 4: The number of being a validator

5.3 Analysis of Node Reputation Value

The reputation evaluation algorithm assigns a reputation value to each node, raising the threshold to become a validator and increasing the cost of malicious behavior. We set node 1 among these 10 nodes to be an honest node which participates in network activities normally. Set node 2 to perform malicious behavior once its reputation value exceeds the initial reputation value RT (RT = 7). Set node 4 to participate in network activities normally but perform malicious behavior occasionally. The reputation values of these three nodes were recorded and the statistical results are shown in Fig. 5.

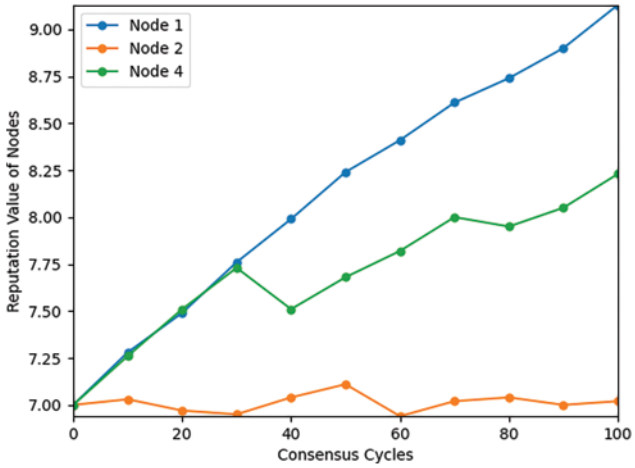

Figure 5: The reputation value of nodes

From the experimental results, node 1 continuously accumulates reputation value because it has been honestly performing network activities. The reputation value of node 1 is significantly higher than that of node 2 and node 4. Node 2 starts to behave maliciously once its reputation value exceeds the initial reputation value, so the reputation value of node 2 is significantly lower than that of node 1 and node 4. Node 4 performs consensus normally in the first 30 consensus cycles, so it performs reputation value accumulation normally like node 1. But after the 30th and 70th consensus cycles, malicious

behavior occurs and the reputation value decreases significantly. In this scheme, the validators are selected from the highest to the lowest reputation value. As long as there are more than $\frac{2}{3}$ honest nodes like node 1 in the network, then nodes like node 2 and node 4 cannot be elected as validators after performing malicious behavior, thus ensuring the security of the system.

6 Conclusion

To address the centralization problem in the PoA consensus mechanism. In this paper, we propose a blockchain consensus mechanism based on dynamic reputation. Aim to the centralization problem in the Proof-of-Authority consensus mechanism, validator as the center of the network, can easily cause harm to the network once it launches an attack on the network. In this paper, we propose a blockchain consensus mechanism based on dynamic reputation. To prevent validators from centralization, a reputation evaluation Algorithm is introduced to dynamically update the reputation value at the end of each cycle. A high reputation node is selected to become the validator in the next cycle, raising the threshold of validator and increasing the cost of malicious behavior. A set of monitoring nodes is selected before the validator generation to monitor the malicious behavior during the consensus of the verification node, and prevent the network from crashing due to the single validator failure. The experiments show that this scheme has stable block-generate time, high consensus efficiency, and can guarantee the fairness of participation in competition among nodes. However, there is still room for improvement in this scheme, and the optimization of node evaluation can be further explored, because if a node performs malicious credit evaluation, there may be different results for node credibility.

Funding Statement: This work is supported by the Key Research and Development Project of Sichuan Province (No.2021YFSY0012, No. 2020YFG0307, No.2021YFG0332), the Key Research and Development Project of Chengdu (No. 2019-YF05-02028-GX), the Innovation Team of Quantum Security Communication of Sichuan Province (No.17TD0009), the Academic and Technical Leaders Training Funding Support Projects of Sichuan Province (No. 2016120080102643).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," April 10, 2018. [Online]. Available: http://bitcoins.info/bitcoin.pdf.

[2] M. Guerar, A. Merlo, M. Migliardi, F. Palmieri and L. Verderame, "A fraud-resilient blockchain-based solution for invoice financing," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1086–1098, 2020.

[3] N. S. Alghamdi and M. A. Khan, "Energy-efficient and blockchain-enabled model for internet of things (IoT) in smart cities," *Computers, Materials & Continua*, vol. 66, no. 3, pp. 2509–2524, 2021.

[4] P. Wang and W. Susilo, "Data security storage model of the internet of things based on blockchain," *Computer Systems Science and Engineering*, vol. 36, no. 1, pp. 213–224, 2021.

[5] C. C. Agbo, Q. H. Mahmoud and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, pp. 56, 2019.

[6] A. I. Khan, A. Saad, F. J. Alsolami, Y. B. Abushark, A. Almalawi *et al.,* "Integrating blockchain technology into healthcare through an intelligent computing technique," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 2835–2860, 2022.

[7] E. A. Akkoyunlu, K. Ekanadham and R. V. Huber, "Some constraints and tradeoffs in the design of network communications," in *Proc. ACM*, New York, NY, USA, pp. 67–74, 1975.

[8] L. Lamport, R. Shostak and M. Pease, "The Byzantine generals problem," in *Proc. ACM*, New York, NY, USA, pp. 382–401, 1982.
[9] S. King and S. Nadal, "PPCoin: Peer-to-peer crypto-currency with proof-of-stake," August 19, 2012. [Online]. Available: https://archive.org/details/PPCoinPaper.
[10] P. K. Singh, R. Singh, S. K. Nandi and S. Nandi, "Managing smart home appliances with proof of authority and blockchain," in *Proc. Innovations for Community Services*, Cham, pp. 221–232, 2019.
[11] U. Chikezie, T. Karacolak and J. C. Do Prado, "Examining the applicability of blockchain to the smart grid using proof-of-authority consensus," in *Proc. SEGE*, Oshawa, Canada, pp. 19–25, 2021.
[12] N. A. Asad, M. T. Elahi, A. A. Hasan and M. A. Yousuf, "Permission-based blockchain with proof of authority for secured healthcare data sharing," in *Proc. ICAICT*, Dhaka, Bangladesh, pp. 35–40, 2020.
[13] G. Li, J. H. Zhang and J. M. Zhan, "Research on blockchain system of improved PoA consensus mechanism for solving issue of phonily occupating seats of civil aviation," *Application Research of Computers*, vol. 37, no. 11, pp. 3368–3372, 2019.
[14] S. D. Kamvar, M. T. Schlosser and H. G. Molina, "The eigentrust algorithm for reputation management in P2P networks," in *Proc. ACM*, New York, NY, USA, pp. 640–651, 2003.
[15] L. Xiong and L. Liu, "PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, no. 7, pp. 843–857, 2004.
[16] J. Zhou, J. Zhang, S. Yan and R. Qu, "Study on consensus mechanism of block chain motivation based on dynamic trust," *Application Research of Computers*, vol. 38, no. 11, pp. 3231–3235+3248, 2021.
[17] J. H. Huang, X. Xu, Z. C. Li, J. H. Li and H. Zheng, "Proof of trust: Mechanism of trust degree based on dynamic authorization," *Journal of Software*, vol. 311, no. 13, pp. 309, 2019.
[18] X. Han, Y. Yuan and F. Y. Wang, "A fair blockchain based on proof of credit," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 5, pp. 922–931, 2019.
[19] M. T. de Oliveira, L. H. A. Reis, D. S. V. Medeiros, R. C. Carrano, S. D. Olabarriaga *et al.,* "Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications," *Computer Networks*, vol. 179, no. 4, pp. 107367, 2020.