A Weak Centralized Consensus Mechanism with More Incentive Effects

Yuxiang Mu, Wanghu Chen, Xiaoyan Liang and Yaqiong Gao

College of Computer Science and Engineering, Northwest Normal University, Lanzhou, 730070, China
1E-mail: 1078927193@qq.com and Tel: 18809461496

Abstract. In the blockchain system, the consensus mechanism not only helps the nodes maintain data consistency, but also has certain functions for token issuance and attack prevention. Aiming at the problems of low enthusiasm and weak centralization in Delegated Proof of Stake (DPoS), this paper proposes a weak centralization consensus mechanism with more incentive effect. We replace the voting link with opportunity verification mechanism, and make the voting link that affects the enthusiasm of nodes become the embodiment of their own rights and interests, so as to strive for the maximization of their own interests. And we also introduce the method of random guess to make the selection of representative nodes more random, so as to achieve the situation of weaker center. At last, combined with the existing problems, the paper analyses the feasible solution with this mechanism.

1. Introduction

In 2008, Satoshi Nakamoto proposed an electronic cash—bitcoin [1] that can be directly paid point-to-point without an intermediary. With the development of technology, blockchain, the underlying technology of Bitcoin, is also known to everyone. The blockchain has attracted wide attention in academia and related application industries due to its decentralization, difficult to tamper, and de-trusting.

As a distributed accounting system, blockchain is a technical solution for collectively maintaining a reliable database by de-centralizing and de-trusting [2]. Essentially, it is a distributed ledger. In the system, each node needs to keep the same ledger. In the non-central environment of the blockchain, how to ensure that each node has the same book, and the consistency of the book data is the primary problem to be solved. In this case, it is necessary to learn from the algorithm realizing state consensus in the distributed system to determine the mechanism of selecting the accounting node and to ensure the consistency of the book data in the whole network.

Consensus refers to the process which several independent parties reach an agreement on a certain issue. Consensus is the premise of cooperation, and cooperation is the foundation of a win-win situation. Only on the premise of reaching an agreement on a certain issue, can each participant cooperate more effectively, so as to ensure the maximization of their own interests. In the blockchain, consensus refers to the consistency of each node to a certain block in an open distributed network [3]. The blockchain consensus not only helps the nodes maintain data consistency, but also has certain functions for token issuance and attack prevention [4]. In the blockchain environment, through the token incentive in the consensus mechanism, the node's own interests are fully guaranteed, and the enthusiasm of the nodes to participate in the system operation is mobilized, so that each node spontaneously maintains the system operation. However, the current incentive mechanism is not perfect. In the Bitcoin proof of work mechanism, the major mining pools have caused the
concentration of computing power, which is returning to the center. In the Delegated Proof of Stake mechanism, the enthusiasm of each node to participate in the voting has great influence on the mechanism. In the view of above problems, this paper proposes a new consensus mechanism, which not only fully mobilizes the initiative of nodes, but also promotes the fairness of nodes and forms a weaker centralized situation.

2. Related Work
In the blockchain system, the consensus mechanism must ensure the consistency of the node data and reward the contribution made by the node. At present, relevant scholars have done a lot of researches on consensus algorithms, and most of them have been used in blockchain application scenarios. There are two major categories of mainstream consensus mechanisms, one is deterministic consensus and the other is probabilistic consensus [5].

2.1. Deterministic Consensus
In the deterministic consensus mechanism, the traditional distributed consistency algorithm is the main one. The main process of this kind of consensus algorithm is to write after the consensus, which means they first vote to elect the representative, then let the representative write content, and others follow. It mainly includes the classic Byzantine problem and its variants. The literature [6] proposed the Paxos algorithm to maximize the consistency of the distributed system from the engineering point of view. The Raft algorithm proposed in the literature [7] is a simplified implementation of the Paxos algorithm. The literature [8] proposed PBFT, practical Byzantine fault tolerance, as long as more than 2/3 nodes in the system work properly, it can guarantee the consistency. This type of algorithm can quickly reach a consensus, but as the number of nodes increases, performance will decrease and the number of nodes cannot be changed at will.

2.2. Probabilistic Consensus
In a probabilistic consensus mechanism, as long as the node has accounting capabilities, it can initiate a billing request. Its consensus process is written first and then consensus, and the number of nodes can be changed at will. The more nodes there are, the more stable the system will be. This kind of mechanism is mainly PoW, PoS, and their improvement mechanism [9].

Literature [10] elaborated on the Proof of Work (PoW) mechanism, which was firstly adopted in the bitcoin system to reach the consensus. Its advantage is that it can solve the problem of data consistency in a completely open and free network. However, this mechanism requires a lot of computing power and other resources, and it takes a long time to achieve data consistency, usually 10 minutes, which is difficult to meet common business needs.

In order to avoid the problem that miners' participation enthusiasm decreases due to the decrease of rewards in the bitcoin system [11], literature [12] proposed Proof of Activity (PoA), which rewards the active node on line. Decred is now the only digital currency using the PoA.

In view of the resource waste and the long consensus time, the literature [13] proposed the Proof of Stake (PoS). Compared with the PoW, this mechanism reduces the resource consumption caused by mathematical operations, and introduces tokens to shorten the time for consensus. However, one of the drawbacks of the mechanism is that it inevitably leads to a monopoly situation, which the multi-stakeholder will enjoy more rights [14]. The other is the loss of the nodes balance, because the probability of being selected by the person with more interests is far greater than that with less interests.

Literature [15] proposed Delegated Proof of Stake (DPoS). This mechanism is similar to the people's congress system. It no longer requires the majority of all the participating nodes to pass the consensus process, but delegates some representatives to do that. This can further improve the efficiency of consensus and better deal with the problem that the system nodes are not online. Because only some of the nodes represent consensus, this kind of mechanism advantage is speed of high efficiency, but it also inevitably brings about negative effects. It will elect nodes with high credibility and the nodes with high credibility will be elected more easily. So repeatedly, the final voting node will become a relatively fixed number of nodes, which is returning towards centralization. Moreover,
in the process of voting, the nodes need to spend time, energy, technology, etc., but the return of voting is very low, so it cannot fully mobilize the enthusiasm of the node voting. In view of the weak center and the low participation of the nodes in the DPoS mechanism, this paper proposes a weaker central consensus mechanism with more incentive effects. In this paper, the voting link in DPoS is replaced by the opportunity verification mechanism, and the verified nodes can become the quasi-representative and obtain the corresponding reward. The voting link that affects the participation becomes the embodiment of the node's own rights and interests. In this way, the nodes are stimulated to increase the enthusiasm of the nodes to participate in the system operation. On the basis of the quasi-representative, the random guessing process is added to ensure the fair random selection of each node. And the corresponding incentive and punishment measures are introduced to make the selected nodes transform dynamically so as to achieve the purpose of weaker center. Thus, a consensus mechanism with incentive effect and weaker center is formed.

3. Weak Central Consensus Mechanism with Incentives

In the Delegated Proof of Stake (DPoS), each node votes to elect a node with higher credibility as a decision maker in the process of reaching consensus. First of all, in the voting process, each node needs the investment of time, energy and technology, but the return of voting is very low. Therefore, the initiative of nodes to participate in system operation cannot be guaranteed. Then, in the process of consensus decision-making, consensus is carried out by nodes with high credibility, which is equivalent to voting a representative layer on a decentralized basis to realize the consensus. If they can be selected as representatives, it means that they have high credibility. Only those with high credibility can be voted as representatives. In the long run, the nodes of the representative layer will become a relatively fixed number of nodes, which is equivalent to a central link.

Therefore, based on the DPoS, this paper proposes a weak central consensus mechanism with more incentive effects. The consensus of this mechanism is carried out in rounds every time. The consensus representative is selected by the opportunity verification mechanism rather than by voting at each node. And the corresponding rewards and punishments have been added to ensure that the nodes of the competition representatives are dynamically changed, thus forming a situation in which the nodes of the representatives are cyclically replaced. On this basis, a method of random guessing number is introduced, so that each round of nodes has the same opportunity to become the representative and make the final consensus decision.

The consensus process of this mechanism is divided into two stages, including the selection of consensus representatives and the distribution of rewards. In the selection process of the first stage consensus representatives, nodes need to pass three layers of screening to become representatives. The first layer is the initialization of the nodes, which ensures that each node has the same rights and interests. The second layer is the process of opportunity verification and the formation of quasi-representatives. Each initial node carries out opportunity verification and forms quasi-representatives when corresponding verification conditions are met. The last layer is the random guessing number and the formation process of the representative. Each quasi-representative verified by opportunity verification will guess a number randomly. And the nodes satisfied with the guessing rule will become the representative and carry out the current consensus decision. The second stage is the reward and punishment in the process of consensus. The fee for all transactions that have reached consensus in this round is awarded to the consensus representative written the block and the quasi-representative nodes participating in the verification. The opportunity impact factors of all quasi-representative nodes are adjusted so that all nodes are at the same level in the next round of competition.

4. The Generation Strategy of Consensus Representatives

The process of generating consensus representatives is divided into three layers. The first is the initialization layer S, which is composed of all the added initial nodes. The nodes of this layer have the same status and equal power. Secondly, the quasi-representative layer C is composed of nodes that meet the opportunity verification. Finally, the representative layer D is used for the final consensus decision, which forms the representative layer through the random guessing number process.
4.1. Initial Layer

The initial layer consists of new nodes that have just been added to the system and old nodes that are ready for the next round of validation. The old nodes may be the quasi-representative nodes that did not become the representative in the previous round, or the representative node that completed the consensus. On the premise of ensuring that the interests of the old nodes are not damaged, all nodes in this layer are made to have equal status and compete fairly in the next round by guaranteeing fair reward distribution measures.

4.2. Quasi-Representative Layer

In the distributed blockchain environment, each node is independent but needs to cooperate with each other. How to attract every node to participate in cooperation is an important part in the blockchain system. A distributed, self-organizing member can participate in collaboration, receive rewards, and consume services provided by the system. It means that it is an employee, a shareholder and a consumer. Such a positive feedback incentive mechanism will greatly improve the stability and security of the system.

Therefore, in the second layer, the opportunity verification method is adopted to replace the original voting link, so that the voting link that affects the node's participation in enthusiasm becomes the embodiment of the node's own rights and interests, which improves the enthusiasm to participate in the system operation.

First we give the following definition:

1) The effective time for the node to participate in running in the system is t, then

\[ t = T_e - T_s \]

Where \( T_s \) represents the initial moment when the node participates in the system operation; \( T_e \) represents the moment when the node performs verification.

2) The valid balance for the node is \( c \), then

\[ c = c_e - c_s \]

Where \( c_e \) represents the number of balances at the end of the previous round; \( c_s \) represents the beginning.

3) The opportunity of the node is \( O \), then

\[ O = A \times t + B \times c \]

In this paper, the rights and interests of nodes are quantified as the weighted sum of running time and balance changes, which are expressed in the form of opportunities. Where A and B are constants and satisfy A+B=1, usually A and B take a value of 0.5.

4) The verification difficulty is Target, which can be set to the corresponding initial value according to different business scenarios. Target is a dynamic quantity that adjusts itself each round. The adjustment process of Target is as follows:

\[ Target = Target \times \frac{m}{n} \]

Where m represents the number of nodes that actually satisfy the opportunity verification, and n represents the number of nodes that theoretically satisfy the opportunity verification. The value of n can be determined according to the number of different interest groups in the system. In theory, it is guaranteed that at least one node of each interest group can pass the verification.

After each round of validation, the Target value is adjusted to prepare for the next round of validation. When the Target value is determined, each node performs verification spontaneously according to its own opportunity \( O \). The condition that the node satisfies the opportunity verification is

\[ O > Target \]

Then, the process of node opportunity verification is shown in method 1:
Method 1: opportunity verification mechanism

**Input:**
- S - Initial node set
- n - The number of nodes the theory satisfies the verification

**Output:**
- C - Quasi-representative node set

1: for each \( s_i \in S \) do
2: \( t \leftarrow t_e - t_S \)
3: \( c \leftarrow c_e - c_S \)
4: \( O \leftarrow c \times t \)
5: \( m = 0 \)
6: if \( O > \text{Target} \) then
7: \( C \leftarrow C \cup \{S_i\} \)
8: \( m \leftarrow m + 1 \)
9: end if
10: end for
11: \( \text{Target} = \text{Target} \times \frac{m}{n} \)
12: return \( C \)

In method 1, the node compares its own rights and interests with the Target value. If the conditions are satisfied, it can become a quasi-representative and enter into the quasi-representative layer C. The node that does not satisfy the condition remains in the initial layer S. After each round, the Target value is adjusted according to the number of quasi-representatives m.

4.3. Quasi-Representative Layer

In order to ensure the fairness of nodes in the quasi-representative layer, the random guessing method is introduced in the third layer of this paper, so that the representative can be randomly selected to achieve the effect of weak center. The m nodes of the quasi-representative layer make random guesses in any range, and each quasi-representative has only one chance to guess in each round. When the random guessing is completed, the broadcast is performed at the quasi-representative layer to make each quasi-representative obtain as many results as possible from the current round of guesses. In all the guessing results, the node corresponding to the median\(^1\) can be the representative to make the final consensus decision. In the process of quasi-representative guessing, each node is opaque and independent from each other. Therefore, selecting the node corresponding to the median can guarantee the randomness of the selection. In this case, the generation of representatives will be more transparent and reduce the possibility of cheating.

Considering the problem that the nodes in the broadcast process cannot completely receive all random numbers due to network delay, this paper adopts the method of verification confirmation number to solve it. For \( \forall c_i \in C \), \( c_i \) receives the set of random numbers \( \{k_1, k_2, \cdots, k_i, \cdots, k_n\} \), \( n \leq m \), we suppose that \( k_i \) is the random number guessed by \( c_i \) and is also the median in the random number sequence it receives. Then \( c_i \) broadcasts to the quasi-representative layer C that he will become the representative \( d_i \), and after receiving the confirmation information of 2/3m quasi-representatives in the quasi-representative layer D, it can become a representative.

Each quasi-representative node except the representative need to verify the legitimacy of the generated block by the representative node. It mainly includes two-part verification: the first verification represents whether the node cheats when it passes the opportunity verification; the second

\(^1\) The median is the number in the middle of a sequential set of data.
verification represents whether the random number guessed by the node is the median of all the results. The enthusiasm of each quasi-representative to participate in the verification directly affects the benefits of the later awards.

5. Rewards and Punishments in The Process of Consensus

After the consensus in each round, rewards will be distributed according to the contributions of each node in this round. The main source of reward is the fee for all transactions in the agreed block in this round. The rewards are mainly distributed to the representatives of the block written in the current round of consensus and the quasi-representatives participating in the verification. Due to the existence of rewards, each node will actively participate in the verification and strive for a greater reward.

Due to the rewards of this round, each node that becomes the quasi-representative will have a relatively larger right and a higher probability of being elected in the next round. In order to avoid the situation that the same nodes are selected repeatedly in each round so as to form a stable quasi-representative layer, the effective time $T$ of all nodes entering the quasi-representative layer will be cleared, this is to say we set the initial time $t_s$ to the time $t_e$ at which the verification ends.

For nodes that failed to pass the opportunity verification in the last round, as the system time keeps increasing, their effective time running in the system will also increase. For the quasi-representatives and representative nodes, although they receive the reward, their effective running time will be reduced. According to the verification method of opportunity verification, in the next round of election, opportunities at all nodes will still be in a relatively balanced situation, which ensures that each node can be relatively fair for the next round of the election.

6. Mechanism Assessment

To evaluate the proposed weak central consensus mechanism of safeguard incentive by means of comparative analysis. On the one hand, it compares with the existing consensus mechanism and analyzes the advantages and disadvantages of this mechanism (see table 1). On the other hand, combined with the current problems, the countermeasures of this mechanism are given (see table 2).

| Table 1. Compare with the main existing algorithms |
|-----------------------------------------------|
|                | Expansibility | Resource Consumption | Efficiency of Consensus | Participation Enthusiasm | Degree of Decentralization |
|---------------|---------------|----------------------|-------------------------|--------------------------|-----------------------------|
| PoW           | Good          | High                 | High                    | Low                      | High                        |
| PoS           | Good          | Middle               | Middle                  | High                     | Middle                      |
| DPoS          | Good          | Low                  | High                    | Middle                   | Low                         |
| PBFT          | Bad           | Middle               | Middle                  | Middle                   | Middle                      |
| This mechanism| Good          | Low                  | High                    | High                     | High                        |

Table 1 compares the model with the existing research results from five aspects. Overall, the model has certain advantages. The mechanism has strong scalability and low resource consumption. The mechanism introduces the rewards and punishments to stimulate the enthusiasm of participation, and adopts the random guess to achieve the effect of a weaker center.
Table 2. Existing Problems and Solutions

| Forms                  | Facing Problems                                                                 | Solution                                                                                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security              | Form a group to influence the guessing results in the guessing stage            | Before guessing the number, it needs to go through the opportunity verification mechanism, which can prove that its impact factor is relatively large. After the consensus is completed, their impact factors will be cleared, which will affect their future verification. Most of this round's rewards went to the final delegate. So the cost of cheating far outweighs the benefits. |
| Expansibility         | What happens to a node that just joined the system?                             | In the action of the initial layer, the nodes newly added to the system have the same verification impact factor, which can be verified fairly.                                                                 |
| Participation         | Where is the driving force for each node to participate in the operation?       | Each node actively participates in the verification and strives for greater rewards through its own rights and interests to maximize its own interests                                                                 |
| Enthusiasm            |                                                                                  |                                                                                                                                                                                                       |
| Resource Consumption  | What resources are consumed to participate in the operation                     | The nodes participating in the operation need to pass the opportunity verification mechanism, and the influence factor of the opportunity verification mechanism is only the running time and balance of the nodes, so the resource consumption is very small. |

Table 2 analyzes the solution of the model for existing problems. The results show that the mechanism has low resource consumption, strong scalability, and can resist certain security attacks. But there are still many flaws and areas that need to be optimized, such as no machine learning ability, no predictive ability and so on.

7. Conclusion
In this paper, a weak centralized consensus mechanism with more incentive effects is designed. In view of the low voting enthusiasm and the weak centralization in the DPoS mechanism, we replaces its voting process with the opportunity verification mechanism and adds random guesses. With the action of the incentive mechanism, it not only improves the participation of the nodes, but also ensures the fairness of the nodes and achieves the effect of a weaker center.

As the core of blockchain, consensus mechanism has attracted more and more attention. In order to make blockchain suitable for the industry, there must be a consensus algorithm suitable for this scenario. The next step will be to propose a consensus algorithm that applies to the corresponding application scenario.

8. Acknowledge
This work is supported by the National Natural Science Foundation of China (No. 61462076).

9. References
[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [J]. 2008.
[2] He Pu, Yu Ge, Zhang Yan-feng, et al. Survey on Blockchain Technology and Its Application Prospect. Computer Science [J], 2017, 44(4):1-7.
[3] Zhang Yong, Li Xiao-hui. The research and implementation of an improved blockchain's consensus mechanism. Electronic Design Engineering [J], 2018, 26(1):38-42.

[4] Duan Xi-nan, Yan zhi-wei, Gen Guang-gang, et al. Research and Trend Analysis on Blockchain Consensus Algorithm. E-Science Technology & Application [J], 2017, 8(6):43-51.

[5] Zheng Z, Xie S, Dai H, et al. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends[C]// IEEE International Congress on Big Data. 2017.

[6] Lamport L. The part-time parliament [J]. ACM Transactions on Computer Systems (TOCS), 1998, 16(2):133-169.

[7] Cunningham E. In the search of an understandable consensus algorithm [J]. Draft of October, 2014.

[8] Castro M, Liskov B. Practical Byzantine fault tolerance[C]/ ACM, 1999:173-186.

[9] Zhou Ye-fei. The evolution of the core technology of blockchain -- the evolution of consensus mechanism. Computer Education [J]. 2017(4):155-158.

[10] Decker C, Wattenhofer R. Information propagation in the Bitcoin network[C]/ IEEE Thirteenth International Conference on Peer-To-Peer Computing. IEEE, 2013:1-10.

[11] Yang Yu-guang, Zhang Shu-xin. Review and Research for Consensus Mechanism of Block Chain. Journal of Information Security Research [J]. 2018(4).

[12] Bentov I, Lee C, Mizrahi A, et al. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [J]. 2014.

[13] Houy N. It Will Cost You Nothing to 'Kill' a Proof-of-Stake Crypto-Currency [J]. Social Science Electronic Publishing, 2014, 34(2).

[14] Zheng Z, Xie S, Dai H N, et al. Blockchain challenges and opportunities: A survey [J]. Work Pap.–2016, 2016.

[15] Han Xuan, Liu Ya-min. Research on the Consensus Mechanisms of Blockchain Technology [J]. Netinfo Security, 2017(9):147-152.