**A New Election Algorithm for DPos Consensus Mechanism in Blockchain**

Yinghui Luo ,YiQun Chen, Qiang Chen

Department of computer science

Guangdong University of Education

Guangzhou, Guangdong, China

e-mail: 13922279101@139.com

Qinglin Liang

Training Center

Guangzhou South China Business Trade College

Guangzhou, Guangdong, China

e-mail: 420697840@qq.com

*Abstract*—The block chain has achieved great success in bitcoin, and its decentralization idea caught highly attention of financial institutions, capital markets and academia. Decentralization is the most fundamental feature of the block chain, but decentralization sacrifices efficiency, while mining leads to high bitcoin transaction costs; in some industries, such as the commercial retail, high efficiency and low cost are required. The consensus algorithm is the core technology to achieve non-centralization. This article proposes a DPoS consensus mechanism election algorithm. This algorithm improves the ring-based coordinator election algorithm. First, the algorithm is used to elect the agents, and then the final winner, reach a new consensus, meet the requirements of the block chain performance in the commercial retail sector, reduce transaction costs, and construct a fair, freely competitive, non-monopoly, secure and non-centralized block chain platform.

Keywords- Block chain; Decentralization;Consensus mechanism ,PoW, DPoS；

# Introduction

## Decentralization has always been regarded by the industry as one of the core attributes of the block chain.

The decentralization of computer systems consists of three aspects:

1. Architectural Decentralization: how many nodes is a system made up of? How many of those nodes can the system tolerate breaking down at any single time?

2. Political Decentralization: How many individuals and organizations do you need to ultimately control this system?

3. Logical Decentralization: Does the interface and data structures that the system presents and maintains look more like a single monolithic object?

From the perspective of architecture, the block chain[1] is based on the peer to peer network, and there is no central controller, so it is decentralized. From a political point, the block chain makes it difficult for a few people to control the entire system through a consensus algorithm, so it is political decentralization. The decentralization of architecture and politics brings three benefits to the block chain: fault tolerance, anti-attack and anti-collusion. However, there is no node in the block chain that can control or coordinate the generation of the book data. Each node coordinates through the consensus algorithm to generate a consistent account book. It is a unified account book of the whole network, so without doubt , it is logically decentralized .

## Pros and cons of decentralization

The following five aspects are the advantages of the decentralization of the block chain:

1. Fault tolerance: Decentralized systems do not depend on a single node. Multiple nodes are dependent on each other that decreases the possibility to fault.

2. Attack protection: Decentralized systems are not centralized. It's hard to attack all nodes of the entire system, because it takes a high price to complete and it is very likely to fail.

3. Prevent monopoly.

4. Prevent collusion.

5. Decentralized development encourages each node to work for itself, thereby increasing the node's obligations and responsibility.

Decentralization is not suitable for all application areas , because it also has 4 major flaws:

1. The decision-making process is slow.

2. Repeated work and useless work: For example, when a node calculates the Hash value of the previous block, the work of other nodes is invalidated.

3. Slow speed: The cost of decentralization is that the processing speed is greatly reduced.

4. The network is under pressure.

By comparison , decentralization may not be the best way to solve all problems[2,3]. It is better not use block chain when you can do the job through centralization.

## Decentralization is determined by the consensus mechanism.

The core of the consensus algorithm is to solve the Byzantine Generals' Problem[4] and achieve the ultimate consistency in the trustless network environment, that is, there are one or more fraudulent nodes in the network, which may intentionally violate the protocol or transmit incorrect data, there is a distributed network consistency problem, the cost is relatively low efficiency. It is the consensus mechanism that determines the degree of “decentralization” of a block chain system. Generally speaking, the higher the degree of centralization, the lower the system efficiency.

To increase the speed of the block chain and reduce energy consumption, the key is to improve its consensus algorithm, which must solve the Byzantine Generals Problem, otherwise it will no longer be a decentralized system.

# Consensus mechanism

The basis of the block chain is the Peer to Peer distributed network, encryption algorithm and consensus mechanism. Among these basic technologies, the consensus mechanism is most important. It can be said that the consensus mechanism is the core of the block chain technology, and the consensus mechanism is its soul for a block chain system. The consensus mechanism largely determines the trust degree among the nodes of the entire block chain system, and also determines the trust degree of other users for the data on the block chain[5].

The so-called "consensus mechanism" is a set of methodologies to enable participants to form a common understanding. It also calls "consensus algorithm". The main ones are:

## PoW: Proof of Work

The algorithm used by the Bitcoin "Consensus Layer" is called PoW, the workload proof mechanism. The specific job is to calculate a special hash value, which is called "mining." This is a Block Hash that meets the requirements. The first N bits are zero. The more the number of zeros, the greater the difficulty value. To get a right Block Hash requires a lot of trial calculations, the calculation time depends on the machine's hash speed. When a node provides a right Block Hash value, it means this node did undergo a lot of trial calculations, because finding a right hash is a probability event. As long as he has completed the workload, and then everyone listens to him, he creates a new block, which is a consensus.

## PoS: Proof of Stake

This kind of mechanism is equivalent to the equity voting system in the company, more shares, more decision-making power.

Fig 1. The topology of POS

## DPoS: Delegated Proof of Stake

DPoS is based on the PoS plus a qualification - election. Similar to the board of directors. The number of board members is limited and elected by everyone. The selected board members can exercise their rights. The member who have voting rights are chosen through election and replacement, rather than by only the amount of coins.

 Fig 2. The topology of DPOS

## comparison PoW and PoS

PoW is an extremely rude original election algorithm, but it very effective to prevent malicious attacks[5].

The biggest problem of PoW currently being criticized is resource consumption, while PoS has no these issues.

Therefore, it can be seen that the biggest difference between PoW and PoS is that PoW does not require too many nodes to communicate and confirm each other under the premise that the algorithm complexity is high enough, and its requirements for the code implementation are extremely low. However, PoS has higher requirements for consistency verification and anti-counterfeiting among multiple nodes, but it can be optimized to a certain level by using the traditional consistency election idea.

## Choice of PoS and DPoS

When using PoS, it must vote among thousands of nodes in the election[6]. The more nodes participating in the cluster, the slower the efficiency, and the greater the pressure on network traffic.

DPoS gives an idea that these thousands of PoS nodes vote among through a mechanism to elect a number of nodes, then vote among these number of nodes , not all nodes in the network, to elect each bookkeeper. This mechanism can greatly improve the efficiency of elections. Consistent voting among dozens, up to hundreds of nodes can generally be done in seconds and reach consensus, so the DPoS mechanism can increase the consensus process to the second level.

As a variant of PoS, DPoS reduces the network pressure by reducing the number of election nodes[7]. It is a typical divide-and-conquer strategy: divide all nodes into leaders and followers, and only inform the followers after reaching a consensus among the leaders. . This mechanism can effectively reduce network pressure without increasing computing resources, and will have strong application value in excellent software implementation[8]. Theoretically, DPoS performance have no upper limit, currently reach hundreds of thousands of transactions per second.

# A new voting DPoS algorithm

The purpose of this algorithm is to select a server among many servers as the generator of the new block. The evaluation criteria of the election are the rights of the candidate. The probability of winning is higher when the rights are bigger. the rights of the candidate are decided by the token amount he owns.

## Basic requirements for algorithm design

First, must meet Byzantine fault-tolerant requirement[9], because the distributed general ledger system of the algorithm that does not solve the Byzantine problem is not a block chain system. Second, in order to reduce broadcast information and avoid network congestion, not all servers in the network are directly involved in elections and being elected. Multiple servers recommend a proxy server to participate in the election; but elections must be fair and prevent monopoly.

## A ring-based coordinator election algorithm

Chang and Roberts [10] propose a distributed computing which is called ring-based coordinator election algorithm.

Fig 3. A ring-based coordinator election algorithm

All nodes are arranged in a logical circular queue, and each node has a unique pre-order node and a post-order node.

Each server has a receiving thread pool and a sending thread pool. When no election is initiated, the two thread pools are blocked until the message arrives to unblock and process the message, and each server has an election thread, a thread that can initiate an election.

As seen in Fig 3, the white server is not a participant in the election, the dark server is the election participant. The Election Message consists of the candidate's ID and its stake value, in order to prevent monopoly, the stake value of any server at the time of election is multiplied by a random number and the winner of the previous session is multiplied by 0 because no node can be re-elected.

## Election process

There are two processes in a complete election. The first is the voting. The initiator starts voting and passes the voting message to the next node. When the message is delivered back to the initiator, all voters can be considered to have voted, then result the winner. The second stage is to broadcast the message of the winner to the whole network and inform all the nodes. The specific process is as follows:

1. Initially each server in the ring is marked as non-participant. Any server can initiate the election process, assuming Node 1 starts an election, it first marks itself as a participant. It multiplies the stake value by a random number to get a new stake value, It creates an election message containing its ID and the new stake value, Then It sends this message clockwise to its next node.

2. When a server receives an election message, if the recipient happens to be the initiator, go to step 3, otherwise:

It compares the stake value in the message with its own stake value. Its own stake value must also be multiplied by a random number.

1).If the stake value in the election message is larger or same, the server unconditionally forwards the election message in a clockwise direction.

2). If the stake value in the election message is smaller, and the server is not yet a participant, the server replaces the stake value and ID in the message with its own new stake value and its own ID, sends the updated election message in a clockwise direction. But when the server is already a participant (ie, the process has already sent out an election message with a ID at least as large as its own ID), the process discards the election message.

3) Repeat step 2).

3, The ID in the Election message is the ID of the winner, The server is winner. The server starts acting as the leader, it begins the second stage of the algorithm.

The leader process marks itself as non-participant and sends an elected message to its neighbor announcing winner’s election and ID.

1).When a server receives an elected message, it marks itself as non-participant, records the elected ID, and forwards the elected message unchanged.

2). When the elected message reaches the newly elected leader, the leader discards that message, and the election is over.

Fig 4 . Algorithm flowchart

# Incentive

In the decentralized system of block chain, all network resources, computing resources and storage resources are provided by users themselves, and each node is both a consumer of the service and a provider of the service. Elections and the generation of new blocks require CPU time, electricity, and network resources. If there is no incentive mechanism, no users are willing to participate, so for each job, such as elections and the generation of new blocks, the provision of each resource, it provides a certain amount of tokens as rewards. At the same time, in order to encourage all nodes to participate together and maintain the safe operation of the block chain system, an equity mechanism is needed as compensation and incentive for participants. That is, through the means of economic balance, to prevent tampering the contents of the general ledger, Token has become an inevitable mechanism for issuing incentives. In addition, this incentive mechanism also encourage nodes to remain honest. If a greedy attacker has the ability to control the bigger power than the full network CPU power of all the honest nodes, and he uses this ability to gain benefits. He will find that it is more profitable to follow the rules of the game. Follow the rules, because breaking the rules will damage the system itself and threaten the effectiveness of his wealth.

# Decentralization and efficiency

## Decentralization of DPoS

The DPoS algorithm uses the witness mechanism to solve the centralization problem, each person holding shares votes, resulting in n-bit representatives(usually n=101), the value of n is decided by the number of nodes on the block chain. the larger number of nodes , the larger the value of n, and the n node representatives share same rights. Due to the decentralized voting mechanism, DPoS is more democratic than other systems. From a certain perspective, DPoS is a bit like a parliamentary system or a people's congress system. If the delegates are unable to perform their duties, they will be delisted and the network will select new super nodes to replace them.

It is not always the node with the largest stake value to be the winner, because that will be easy to cause monopoly and manipulation. Multiplies the stake value of each node by a random number in the election, and prohibit re-election.This electoral system has the following advantages:

The larger the equity , the higher probability of being elected , guarantees the stability of the system.

2. The small equity may also be elected, ensuring the fairness of the system.

3. Certain restrictions is placed on the big equities. ensure that the system is not manipulated and monopolized.

4. Due to the token reward system, the election mechanism effectively prevents the rich from becoming richer.

Through this real-time change of shareholder voting mechanism, this makes the whole system is more like a 24-hour uninterrupted shareholder meeting, and shareholders can change the company's organizational structure at any time by voting. Comparing Bitcoin, the right to vote in the network is firmly in the hands of shareholders, not controlled by a node.

## Avoid hard forks and soft forks

Since the block chain is a decentralized system, the generation of blocks is generated through competition across the entire network. There is no referee or coordinator, the block tends to fork. This is because under an unsound consensus mechanism, nodes have differences. Sometimes multiple nodes succeed in mining at the same time, they all declare themselves as winners. Each winner generates a new block, that’s the forks.

 The other case is that the block chain is a decentralized data structure, different copies cannot always be consistent. It is possible for a block to reach different nodes at different times, resulting in nodes having different block chain perspectives. The solution is that each node always selects and tries to extend the block chain that represents the maximum amount of work proof, that is, the chain with the longest or largest cumulative difficulty, and the other chain will be discarded.

Through the consensus mechanism of elections, block forks can be avoided, as long as only one winner is selected for each election, only one node can generate new blocks, and block forks can be avoided.

## Efficiency of the election algorithm

If the number of people participating in the election is n, the number of rounds of the election process is n times. This process is called the first stage. When the voting is over, the initiator of the election broadcasts the election result to the whole network, , inform each node about who is elected. When the information of last node election result is successfully delivered to the initiator, this is considered as success of the election result broadcast, this process is called the second stage, and it needs to be cycled n times, until the election is completely finished , so the cost of the algorithm is to deliver the messages 2\*n times. If there is any problem in the whole process, it can only be regarded as a failed election, and the election is invalid.

Obviously, the election algorithm only needs to deliver messages and confirm elections. It does not require complicated calculations and can be completed within 1 second. It is much more efficient than bitcoin's PoW algorithm. Compare with the current bitcoin network, it takes about 10 minutes to generate a block. it takes an average of 6 rounds of confirmation, which is 60 minutes to confirm that a transaction really takes place. So the efficiency of election algorithm is greatly improved.

# Conclusions

In this article, the DPoS consensus mechanism is used to implement the block chain. Through two elections, first , elect the representatives, then the generator of the block. The election algorithm uses the improved A ring-based coordinator election algorithm as the consensus algorithm. Ensure the Decentralization of the whole process and the fairness, prevents monopoly. The efficiency of the whole algorithm is much higher than that of PoW, which reduces transaction costs.

On the other hand, since the consensus algorithm proposed in this paper is the block generator elected by the whole network nodes, there is another situation in realities, that is, when a node i initiates an election activity, but the election message has not arrived to all nodes of the entire network, it is possible that another node j initiates an election process without knowing the activities of node i, at the same time, two or more elections will be going on the whole network. Obviously, if this happens, it is impossible for the whole network to reach consensus to select the unanimously recognized block generators, the consensus mechanism will have serious problems. All the algorithms still need to be improved. We will initialize the election environment in the future work. A election start after the consensus reached on the whole network, that will avoid multiple votes at the same time.

##### References

1. Nakamoto, S, “Bitcoin: a peer-to-peer electronic cash system,”

Consulted, vol.1, 2008, pp.2012, doi:10.1126/science.1079329.

1. Shi, E., & Shi, E., “FruitChains: A Fair Blockchain. ACM Symposium on Principles of Distributed Computing,” ACM, July2017, pp.315-324, doi:10.1145/3087801.3087809.
2. Yonatan Sompolinsky and Aviv Zohar, “Secure high-rate transaction processing in bitcoin,” In Financial Cryptography and Data Security, Springer, vol. 8975, July 2015, pp.507–527, doi:10.1007/978-3-662-47854-7\_32.
3. Lamport L. Byzantizing Paxos by Refinement, “Distributed Computing,” Springer Berlin Heidelberg, vol. 6950, 2011, pp.211-224.
4. Ayelet Sapirshtein, Yonatan Sompolinsky, and Aviv Zohar, “Optimal selﬁsh mining strategies in bitcoin,” In Financial Crypto, vol.16, 2016, pp 515-532, doi:10.1007/978-3-662-54970-4\_30.
5. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P., “Blockchain for IoT Security and Privacy: The Case Study of a Smart Home,” IEEE International Conference on Pervasive Computing and Communications Workshops. IEEE, May 2017, doi: 10.1109/PERCOMW.2017.7917634.
6. Juan Garay, Aggelos Kiayias, and Nikos Leonardos, “The bitcoin backbone protocol: Analysis and applications,” In Advances in Cryptology-EUROCRYPT 2015, Springer, vol.9057, 2015, pp.281–310, doi:10.1007/978-3-662-46803-6\_10.
7. Yoad Lewenberg, Yonatan Sompolinsky, and Aviv Zohar, “Inclusive block chain protocols,” In Financial Crypto, vol.8975, 2015, pp 528-547, doi:10.1007/978-3-662-47854-7\_33.
8. Lamport, L., Shostak, R., & Pease, M., “The Byzantine Generals Problem,” ACM, vol.4 (3), 1982, pp.382-401.
9. Ernest Chang; Rosemary Roberts, “An improved algorithm for decentralized extreme-finding in circular configurations of processes,” Communications of the ACM, ACM, vol.22 (5), Jan.1979, pp.281–283.