EasyChair Preprint

№ 2445

# Overview of Blockchain consensus mechanism

Changqiang Zhang



January 22, 2020

# Overview of Blockchain consensus mechanism

*Changqiang Zhang*
Key Laboratory of Parallel and Distributed Computing
College of Computer, National University of Defense Technology
Changsha, 410073, China
charleszcq@foxmail.com

***Abstract*— The advent of the Bitcoin system has brought another boom in the Internet era. In a very short time, many Blockchain systems come into being successively, whose decentration, consensus mechanisms, intelligent contract, and other characteristics make them applicable to various fields such as finance, education, medical, technology, etc. The consensus mechanism is the core of Blockchain technology. And a good consensus mechanism plays a very important role in the stable operation of the Blockchain system. The continuous improvement of consensus mechanisms such as PoW, PoS, DPoS, and PBFT has led to the evolution of Blockchain technology to Blockchain 3.0. Starting from the issue of Byzantine generals, this article analyzes common consensus mechanisms based on existing Blockchain applications and then evaluates their consistency. Finally, the prospect of consensus mechanism development is discussed.**

***Keywords- consensus mechanism; Blockchain; the Byzantine generals problem; PoW; PoS; DPoS; PBFT;***

## I. BLOCKCHAIN AND CONSENSUS MECHANISM

### *A. consensus mechanism*

In distributed computing, the decentralized network will inevitably lead to the distrust among networks. In order to ensure the reliability of the network, the network systems will negotiate through the relevant protocols to reach a consensus, thus achieving consistency. This is the so-called consensus mechanism.

The consensus mechanism is used to solve the consistency problem of distributed systems [1]. Protected by a consensus algorithm, for a limited period of time, a given operation is consistent, acknowledged, and tamper-proof in a distributed network [2]. The essence of consensus algorithm is to solve the trust problem of de-centralization.

The negotiation and determination of consensus mechanism are relatively easy to realize, and voting can be conducted through multicast. However, this process is often affected by many uncertain factors. For example, in a distributed system, the deliberately delayed interruption of some nodes, the processing errors of nodes and the malicious nature of nodes all interfere the effective implementation of the consensus mechanism. Therefore, the efficient operation of distributed systems relies on an effective consensus mechanism.

### *B. The relationship between Blockchain and consensus mechanism*

The generation of the Blockchain system has promoted the efficient development of the consensus mechanism. From PoW consensus mechanism to PoS consensus mechanism, and then to DPoS and PBFT consensus mechanism, the consensus mechanism is gradually improving.

Blockchain was originally proposed due to the emergence of the Bitcoin system. It is the underlying implementation of Bitcoin, which has the advantages of decentralization, anonymity, tamper-proof, security and credibility. Essentially, it is a decentralized distributed ledger. The decentralization is a unique idea brought by the Blockchain technology. In the past, we all live in a centralized environment, often under the monitoring and management of government or some organizations. While in decentralized network environment realized by Blockchain, we don't have a wide variety of centralized organization supervision, but fairness and justice between each node. Consequently, a consensus between each node is needed to realize the legitimacy of the deal and decentralization of Blockchain.

The consensus mechanism is the core of the Blockchain technology. The effectiveness of the consensus mechanism directly determines the stable and safe operation of the Blockchain system. The efficient consensus mechanism enables the Blockchain to form a consistent Blockchain structure through effective negotiation.

### *C. Evaluation of consensus mechanism*

In general, we will evaluate the technical level of a Blockchain consensus mechanism through the following aspects:

- Consistency. The most basic part of the consensus mechanism is to make the nodes reach consensus and maintain consistency, so as to minimize the probability of bifurcation.
- Security. Namely, fault tolerance rate, compares the number of malicious nodes the system can accommodate under a certain consensus mechanism, and determines whether it can prevent attacks such as selfish mining and double payment [3].
- Scalability. Whether it supports the expansion of network nodes, when the addition of new nodes in the network or the increase of the number of conf-irmed nodes on the robustness of the whole system, we can generally be measured by the network thro-ughput.

- Performance efficiency. The number of confirmed transactions per second the system can process.
- Resource consumption. In the process of reaching a consensus, the computational force of the system is the computational resource consumed [3].

### *D. Consensus mechanisms and Byzantine generals problem*

When it comes to the consensus mechanism, the famous Byzantine generals have to be mentioned. In 1982, Leslie Lamport first proposed The Byzantine generals problem in "The Byzantine generals problem" [4]. Located in what is now Istanbul, Turkey, Byzantium was the capital of the eastern Roman Empire. At that time, the Roman Empire was so vast that in order to defend itself against the enemy, the armies were so far apart that communication between the armies could only be carried out through couriers. The army would have to trust the couriers completely, but some of the generals would be traitors who would use couriers to send false messages to confuse the other troops. Because the army is more dispersed, a unified attack or retreat is necessary to gain greater initiative in the war. So, a loyal general must make the right plan, knowing that there are traitors, to get the most out of a war.

In fact, the consensus mechanism solved the problem of Byzantine generals. In a distributed system with numerous scattered nodes, it is necessary to make the numerous nodes negotiate with the knowledge of the disloyal nodes so as to make a correct judgment. The consensus mechanism aims at realizing the verifiability and tamper-resistance of the Blockchain by effectively getting the approval of these nodes

## II. CONSENSUS MECHANISM

### *A. PoW workload proof consensus mechanism*

#### *1) Bitcoin and PoW consensus mechanism*

In 2008, Nakamoto S. Bitcoin published "A peer-to-peer electronic cash system[J]"[5], proposing the PoW consensus mechanism, which belongs to unlicensed consensus. Its core idea is to ensure data consistency and consensus security by competing the computing power of distributed nodes. In the Bitcoin system, every transaction must be recorded in a block, based on that, the transactions could be considered legitimate and unanimously recognized by the nodes.

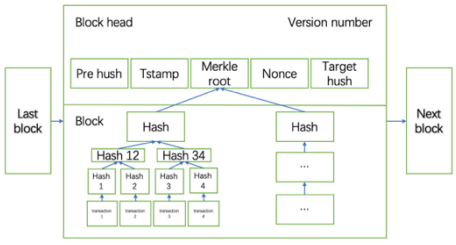


Figure 1. Block structure

Each block in the Bitcoin system usually consists of six parts (figure 1), which are the 4-byte version number, the sha-256 hash value (PreHash) of the previous block, and the Merkle root, Tstamp, Nonce, and Target Hash obtained after verifying all transactionst.

The formation of block is the process of mining, and the specific process is as follows (figure 2):

*a) each node selects a certain number of transactions from the current memory pool.*

*b) verify the legitimacy of the selected transaction, and then package it.*

*c) find a suitable random number for hash calculation so that the hash value is less than the objective function [6]. The solution method is as follows:*

*Hash（PreHash，Mroot，Tstamp，Nonce）<Target*

*d) when an absentee finds a suitable random number, and creates a block, it will be broadcast to the whole network for verification, so as to reach a consensus and acknowledge the validity of the block, so as to store the block content together with the whole network.*

*e) in many cases, different nodes will find the block which meets the requirements at the same time, and then the Blockchain system will appear bifurcation. In such cases, Bitcoin adopts the principle of the longest chain, which requires six more confirmations on the basis of the current block before it can be recognized. In other words, it needs to generate six consecutive blocks that meet the requirements on this block. When one of the bifurcated chains meets the requirements, it becomes the main chain and the other bifurcated chains are cut off.*

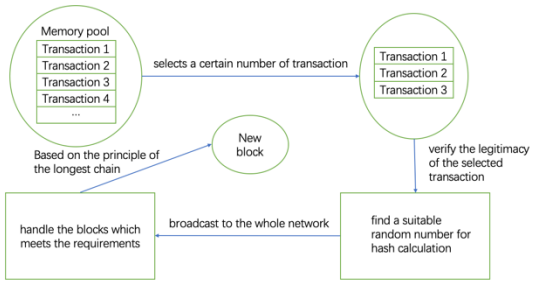


Figure 2. Block formation process

In the process of random number search, absenteeism will continue to try to find a suitable random number which is less than the target value. At the same time the difficulty Target is also updated regularly to keep producing a block every 10 minutes. To encourage absenteeism in mining for random numbers, absenteeism is rewarded with a certain amount of Bitcoin for solving a math problem. Through this incentive mechanism to maintain a significant number of absenteeism mining, the stability of the Bitcoin system can be maintained.

In the Bitcoin system, each node will solve a complicated but easily verified mathematical problem SHA256 based on its own computing power.

#### *2) PoW assessment*

The workload proof mechanism achieves the consensus of the whole network by calculating and solving the difficult problems, which realizes the decentralization, prevents double payment and reaches the agreement of the transaction

in a limited time, thus ensuring the stable operation of the system.

But there are still many shortcomings. Because it is solved by computing power, it consumes a lot of resources. For example, if one miner succeeds in mining, it means that a lot of calculation efforts of other participants will be wasted, which is contrary to our ecological development. Moreover, the transaction confirmation time (consensus reaching cycle) is long and the concurrency is low.

If we combine a large number of nodes to mine, then it will also pose a great threat to decentralization. In July 2017, since a large amount of computing power of Bitcoin was occupied by the Bitcoin continent, and BIP91, the bifurcation scheme of Bitcoin, was supported by the whole network computing power, the hard bifurcation system Bitcoin cash emerged, which once competed with Bitcoin. Today, Bitcoin's top five mining pools together account for more than 50 percent of global computing power[7] which has become one of the insecure factors of the Bitcoin system.

In order to achieve greater computing power, the ASIC mining machine targeted at the SHA256 algorithm of Bitcoin was developed. Under the same power consumption, its computing power was several thousand times that of CPU, which undoubtedly brought about "ASIC", making the Bitcoin system more centralized.

In addition to mechanisms like Bitcoin that use sha-256 algorithms for workload proof, there are also algorithms for workload proof like Litecoin that use "ASIC resistance" scrypt algorithms, scrypt-n, Skein, Groestl, SHA3, X11, and Blake.

### *B. PoS interest proof consensus mechanism*

#### *1) PoS consensus mechanism*

In 2011, Quantum Mechanic proposed the proof-of-stake (PoS) Proof mechanism in Bitcointalk forum.

PoS consensus mechanism is an alternative solution to the resource waste and security defects of PoW consensus mechanism. The POS consensus mechanism uses the equity proof to replace the workload proof based on the hash calculation force in the PoW. The node with a larger interest in the system gains block accounting right. The greater the ownership of a specific amount of currency is, the higher the interest of the node is. The equity is essentially the age of the coin, the number of tokens times the length of the last transaction. In the PoW consensus process, each node has the same difficulty in mining, while in the POS consensus process, the more COINS are consumed, the lower the difficulty in mining and the higher the probability of finding the block. After a block is generated on a node, it is also broadcast to the whole network for verification.

There are very few Blockchain projects that apply to the "pure" equity proof mechanism, and most equity proof mechanisms rely on the varying degrees of workload proof mechanism as a security guarantee. In 2014, Nxt[8] and Blackcoin adopted the POS consensus mechanism, in which Nxt does not adopt the mining mechanism proved by workload.

#### *2) Ethereum and Casper agree mechanism*

In 2013, Vitalik Buterin founded Ethereum[9]. In early 2016, ethereum technology was recognized by the market and ethereum proposed the Casper consensus mechanism based on POS mechanism[10]. The Casper consensus is the result of the migration from the PoW consensus to the POS consensus. Miners had to put the coins into ethereum as collateral, and according to the amount and the time of the coins the pledged, they will get the credits and rewards proportionally. The so-called bookkeeping right is to verify the validity of the transaction. In the process of verification, if the absenteeism is cheating, the system will punish him, confiscate his mortgage tokens and cancel his bookkeeping right. The Casper consensus mechanism virtualizes the mining process and yields blocks when the verified transaction is confirmed by other nodes. Ethereum produces a block every 10 seconds to a minute, increasing the speed of production and reducing the resource waste.

The blocks generated in ethereum are different from those in Bitcoin. The header of ethereum mainly contains the following information: A block of hash value (parent Hash), the predecessor of the block list (ommers Hash), the hash value of the block mining cost account address (benerficiary), state dictionary hash value of the root node (state Root), block all transactions dictionary hash value is the root node (transactions Root), a dictionary that blocks all receipts of the root node hash value (receipts Root), composed of log information filter (logs Bloom), Difficulty level, current block version number, gas Limit for each block, gas Used, timestamp, nonce, mix Hash, etc.

Compared with Bitcoin, ethereum added a status dictionary tree and a receipt dictionary tree to the trans-action dictionary tree in the block. Compared with the trans-action dictionary tree, the status dictionary tree and receipt dictionary tree enable light client nodes to query and verify transactions. It also modifies Merkle tree to Merkle Patricia tree [11], which greatly saves its space and increases the efficiency.

In blocks, etheric lane increases the hash value of the predecessors of the block. Due to the ethereum has increased the average time to get a block out to around 15 seconds and the network delays, a shorter period of time is bound to generate more competition. When a block is follo-wed by six block confirmations, it will be add to the chain, and the production of too many tertiary blocks in a short time is bound to increase the instability of the system. So the purpose of introducing older blocks into the header is to increase the stability of the system by rewarding the abse-nteeism of the generation of these discarded tertiary blocks.

Blocks are divided into difficulty levels, which means the block difficulty level is dynamically adjusted according to the block verification time. When the verification time slows down, the difficulty threshold is also lowered.

#### *3) POS assessment*

The POS consensus mechanism reduces some resource consumption and has good scalability, but it is prone to the risk of bifurcation in high-latency networks[12] . Compared to the workload, it also has a fault tolerant rate of 50%. In June, 2016, as a result of the etheric fang holes, the etheric money worth $fifty million was stolen. To recover losses, the nodes

voted, and after more than 50% of the votes were received, the ethereum maintenance team made a hard-fork change to the ethereum code that, while well-intentioned, was enough to prove that it could not defend against a 50% attack. Due to the use of rights and interests proof mechanism, that is, the greater the interests are, the greater the powers are, which makes the corruption of right-holders inevitable.

### *C. DPoS authorize share certificate consensus mechanism*

#### *1) DPoS consensus mechanism*

The DPoS consensus mechanism is the optimization of PoS, proposed by Bitshares. It selects specific representative-es from a number of nodes in the PoS that hold equity interests and allows them to, in turn, bundle and settle transactions to produce a new block. Each authorized representative node receives revenue from each transaction fee and must pay a deposit to become an authorized representative. The authorized representative must be responsible for other equity nodes. If he or she fails to sign the corresponding block, the nodes will be disqualified.

#### *2) EOS and DPOS consensus mechanism*

EOS[13] use DPoS consensus mechanism, hold the token of the node in the system to vote to select super node block production, its elected 21 super nodes and 100 standby nodes. The order of the 21 nodes should be determined after the negotiation and signature confirmation of at least 15 nodes. During the block production, EOS follows the longest chain principle, which does not allow a node to produce blocks on both chains. If a node misses the production of a block and does not produce a block within the previous 24 hours, it will not be allowed to be produced. The node will generate a block every 0.5 seconds, and the irreversible confirmation of the block only takes 1 second, which greatly improves the efficiency and avoids the efficiency problem of bookkeeping of a large number of nodes, but its centralization problem is serious.

DPoS assessment

In the DPOS consensus mechanism, each node can independently elect its trusted representative nodes, which greatly reduces the number of nodes participating in verification and bookkeeping, so as to conduct consensus verification quickly and greatly improve the transaction speed while saving resources. Compared with the PoW and PoS consensus, DPoS can greatly increase the number of deals accommodated in a single block. In the workload proof and equity proof mechanism, the capacity restriction is the main factor that limits operation speed of the systems. Currently the Bitcoin system can handle only 7 transaction per second [14] , the etheric fang can only handle around 25 deals per second before using subdivision technology [15] , while using DPoS mechanism of EOS can reach millions of level of transactions per second. DPoS mechanism have solved the capacity limitation brought by traditional consensus.

### *D. PBFT Byzantine fault tolerant mechanism*

#### *1) PBFT*

PBFT mainly applies the chain of alliances with the enterprise, which was proposed by Castro and Liskov in 1999. Practical Byzantine Fault Tolerance (PBFT)[16] can tolerate malicious nodes which are no more than one third of the total number. The specific process is as follows:

*a) select a master node in the whole network to be responsible for generating new blocks.*

*b) the master node collects new transactions broadcast by other nodes across the network, sorts them and broadcasts them across the network.*

*c) each node will simulate the transaction execution of the sorted transaction list in order for verification. After the transaction execution, the hash summary calculated by the new block will be broadcast to the whole network.*

*d) if 2*f (f represent the number of tolerated malicious nodes) of the same correct record is received on one node, a commit message is broadcast to the whole network for confirmation.*

*e) if the node receives 2*f+1 commit message, it will be recognized by the nodes and a new block can be formally generated to join the Blockchain.*

#### *2) PBFT assessment*

The Byzantine fault-tolerant mechanism does not compete for computing power, reducing its waste of resources. In the whole network, only one master node is responsible for generating new blocks, and no bifurcation will occur. The remaining nodes only need to be verified, which improves the system efficiency. However, PBFT's fault tolerance rate is only one third, so it cannot prevent witch attacks and its security needs to be improved. If the master node has malicious behavior and proposes an invalid node to the whole network, the block will not be generated and its efficiency will be affected.

Unlike PoW, PoS, and DPoS, PBFT does not require the use of tokens, which is popular in many Blockchain projects, such as the ibm-led hyper ledger project, which uses the PBFT consensus.

## III. IMPROVEMENT OF CONSENSUS MECHANISM

### *A. Selecting a Template (Heading 2)*

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the US-letter paper size. If you are using A4-sized paper, please close this template and download the file for A4 paper format called “CPS_A4_format”.

### *B. Maintaining the Integrity of the Specifications*

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed, please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

## IV. CONCLUSION

The selection of a consensus mechanism is closely related to its applicable application scenario. In the public chain, we can hardly trust each other completely, so we need to use the consensus algorithm with strong consistency, such as PoW, PoS, etc. While in the federation chain, we can use the highly consistent consensus algorithm, such as PBFT, Paxos, Raft, etc., in the case of mutual trust. Only by applying a good consensus mechanism to a suitable scenario can its benefits be maximized.

The quality of a consensus mechanism will directly affect the safe and stable operation of Blockchain projects. Although the consensus of the existing mechanism has solved some of the consistency issues affecting the development of chain blocks, but with the rapid development of network information, people's increasing demand for trading, delayed threat to Blockchain branch network, system fault tolerance rate, network security, right-holders' corruption are problems that we need to solve. An inappropriate consensus mechanism tends to have many hidden drawbacks such as "double take" attack, hard-fork, vulnerabilities, and so on. Therefore, it is necessary to continue to improve the consensus mechanism.

The rapid development of Blockchain requires us to find more efficient consensus algorithm, which contains integrate reward and punishment mechanism to improve system throughput, increase system fault tolerance rate, and to improve system security. Our goal is to make the whole network nodes maintain a high degree of consistency, and to make Blockchain truly benefit mankind.

## REFERENCES


[1] 王晓光.区块链技术共识算法综述[J].信息与电脑，2017(9)：72-74

[2] Antonopoulos A. Mastering Bitcoin. 2015.

[3] 韩璇，刘亚敏．区块链技术中的共识机制研究 [J]. 信息网络安全, 2017（9）：147-152.

[4] Lamport L. Shostak R, Pease M. The byzantine generals problem[J].ACM Trans on Programming Languages and Systems, 1982, 4(3):133-169

[5] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2009.

[6] Antonopoulos AM. Mastering Bitcoin: Unlocking Digital Crypto-Currencies. Oreilly Media Inc Usa, 2015.

[7] 比特币矿池全球算力分布 [EB/OL]. http://www.btcker.com/pools/.

[8] Nxt Whitepaper, 2014. https://www.dropbox.com/s/cbuwrorf672c0y-y/NxtWhitepaper_v122_rev4.pdf

[9] Buterin V. A next-generation smart contract and decentralized application platform [J]. Etherum, 2014(1):1-36.

[10] Danny R. Casper proof of stake FAQs[EB/OL]. (2018-08-02). https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs

[11] Morrision D R. PATRICIA—Practical algorithm to retrieve information coded in alphanumeric. Journal of the ACM,1968,15(4):514-534.

[12] 周邺飞.区块链核心技术演进之路--共识机制演进(1).计算机教育,2017(4)：155-158

[13] EOS.IO Technical WhitePaper v2, [EB/OL] (2018). https://github.com/EOSIO/Documentation.

[14] Wattenhofer R. The Science of the Blockchain. Charleston, USA: CreateSpace Independent Publishing Platform, 2016.

[15] Buterin V. Ethereum 2.0 mauve paper. White Paper. 2016.

[16] CASTRO M, LISKOV B. Practical Byzantine Fault Tolerance[EB/OL].https://wenku.baidu.com/view/3cc69308bb68a98271fefa38.html.

[17] Ren L.Proof of stake velocity: Building the social aurrency of the digital age [EB/OL].2014[2018-03-23].http://www.reddcoin.com/papers/PoSV.pdf

[18] 杨宇光,张树新.区块链共识机制综述[J].信息安全研究,2018(4)：369-379.

[19] DUONG T, FAN Lei, ZHOU Hongsheng. 2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely[EB/OL]. http://eprint.iacr.org/2016/716.pdf,2017-4-15.

[20] CHEN Jing, MICALI S. Algorand[EB/OL]. http://arxiv.org/abs/1-607.01341,2016-7-5.

[21] Popov S. The tangle. White Paper,2016

[22] What is Proof of Authority Consensus? Staking Your Identity on The Blockchain. https://blockonomi.com/proof-of-authority.

[23] Internet of Services: The Next-generation, Secure, Highly Scalable Ecosystem for Online Services, 2017.https://github.com/iost-official/-Documents/blob/master/Technical_White_Paper/EN/Tech_white_paper_EN.md.

[24] Why Proof-of-Capacity could be the future of cryptocurrency.https://-minergate.com/blog/why-proof-of-capacity-could-be-the-future-of-cryptocurrency.

[25] NulsWhitepaper1.1.https://nuls.io/pdf/NulsWhitepaper1.1.pdf.

[26] NEM Technical Reference. https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf

[27] Nebulas Technical White Paper. https://nebulas.io/docs/NebulasTechnicalWhitepaper.pdf.

[28] The Thunder Protocol. https://docs.thundercore.com/thunder-whitepaper.pdf.

[29] POSW-Proof of Shared (or Standardized) work. https://hackernoon.com/proof-of-rental-or-shared-work-d7150965edf6.