2022 International Conference on Data Analytics, Computing and Artificial Intelligence (ICDACAI) | 978-1-6654-5470-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICDACAI57211.2022.00098

Analysis on Blockchain Consensus Mechanism Based on Proof of Work and Proof of Stake

Shi Yan
Wuhan University
Wuhan, China
2020302181047@whu.edu.cn

***Abstract*—In the white book of Bitcion, Satoshi Nakamoto described a bitcoin system that can realize point-to-point online payment without a third-party organization. After supporting this magical application scenario and subverting the traditional centralized system, the blockchain technology has attracted worldwide attention, triggered a research upsurge of blockchain consensus algorithm, and produced a large number of innovative applications. Although various consensus algorithms continue to evolve with the iteration of blockchain products and applications, Proof of Work (POW) and Proof of Skake (POS) algorithms are still the core of consensus algorithms. This paper discussestwo algorithms of POW and POS in blockchain consensus mechanism, and analyzes the advantages and the existing problems of the two consensus mechanisms. Since consensus mechanism is the main focus of blockchain technology and has many influencing factors, this paper discusses the current problems and some improved ideas, and selectes some typical algorithms for a more systematic introduction. In addition, some important issues related to safety and performance are also discussed. This paper provides the researchers a great reference on blockchain consensus mechanism.**

***Keywords*—Blockchain, Proof of Work, Proof of Stake, Nothing-at-stake Attack, Consensus Mechanism**

I. Introduction

Since the emergence of bitcoin [1,2] system in 2009, its underlying blockchain technology has gradually attracted the attention of academia and industry, and has achieved rapid development. At present, blockchain technology has been widely used.

In the traditional network, the reliability of the online payment platform, such as WeChat and Alipay, is determined by the provider of the business system. The security of personal identity information and transaction records also depends on the reputation and security of the third party organizations. This centralized business processing mode has been broken in the blockchain system. With the brief description of bitcoin principle in Nakamoto's study[1] on November 11, 2008, as well as the official launch of bitcoin system and the advent of Genesis block in 2009, the bitcoin system has been developing tepidly for nearly 10 years. After that, people find that through the underlying technology of blockchain, it can realize the same function in a completely decentralized environment, compared to the traditional centralized environment. The key to complete this function is the consensus algorithm.

The core of the consensus mechanism is to solve the problem of consistency in the distributed system through the consensus algorithm, so that each node can be recognized and cannot be tampered with. In the blockchain system, it mainly solves the consistency of transaction data and transaction status of each node in the distributed system, and realizes decentralized multi-party mutual trust. Consensus algorithm is the core technology of blockchain and the key technology to realize the Internet from information interconnection to value interconnection.

Blockchain can be divided into public chain and license chain according to node permissions. Public chain means that blockchain nodes have no access mechanism and participating nodes can join or exit at any time. There are two representative consensus algorithms.One is proof of work (POW), which is the probability of obtaining rights by consuming computing power. The greater the computing power is, the higher the probability can be. Its advantages are the strong randomness and great fairness, while its disadvantages are energy consumption and low consensus efficiency. The second is the proof of stake (POS), which is the probability of obtaining rights by holding assets. The more assets are, the greater the probability can be. Its advantage is energy conservation and environmental protection, while the disadvantage is power concentration.

As for the consensus mechanism which is core of blockchain technology, this paper aims to discuss the POW and POS mechanisms in the blockchain consensus, and the advantages and the existing problems of the two consensus mechanisms based on the relevant studies.

II. Different Types of Consensus Mechanisms

A. Proof of Work

1) Hashcash: inspiration for proof of work

Proof of work(POW) for Bitcoin blockchain borrows the idea of Hashcash, which was proposed to deal with the issues of junk email in May, 1997 [3]. In junk email, an attacker almost costs nothing. Software of junk email can send emails in batches to the destination address. Hashcash can solve these problems by making attackers consume some computing resources.

To be detailed, the messages of email sent by the sender must contain a signature consisting of the recipient's address, sending time, and counter. The counter is supposed to make the signature meet the conditions. The SHA-1 algorithm should be used to generate a 160 bits-long hash value for the signature, the first 20 bits of which are all zero. As a result, before sending a message, the sender needs to constantly adjust the counter value to generate a qualified email signature, while the mail server only needs to perform SHA-1 calculation once to judge whether the signature meets the conditions.

2) Concept of POW

978-1-6654-5470-4/22/$31.00 ©2022 IEEE
DOI 10.1109/ICDACAI57211.2022.00098

The concept of POW was first proposed by Jakobsson in 1999 [4]. POW is used to achieve verifiable computing tasks. It includes two sides: certifier and verifier. The certifier provides evidence to the verifier to show that it has completed a number of calculations in a period of time. Since the generation of evidence requires amount of computing resources, POW can be used to solve denial of service (DOS) attacks.

In bitcoin network[1], given a value D, there is a block contains all transaction data. Miners should calculate the 'nonce' so that the value calculated by SHA-256 twice is less than D, as presented as Formula 1:

$$\mathrm{SHA256}\big(\mathrm{SHA256}(\mathrm{data}||\mathrm{nonce})\big) \le \mathrm{D} \qquad (1)$$

In that case, the miner can win the competition only by constantly changing the input nonce value[5]. Figure1 shows nonce in blockchain node. It is determined by the computing power of the miner, so the competition of POW finally turns to the competition of hash computing power in bitcoin network[5]. In addition, the value D can change to adjust the difficulty of mining[1].

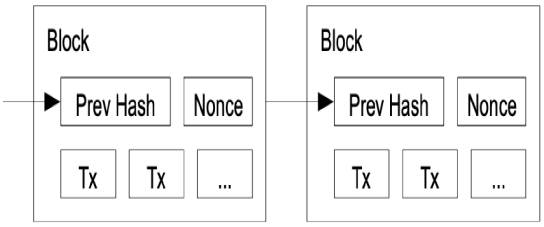

Fig. 1. Nonce in blockchain node[1]

The adjustment of difficulty value occurs automatically in each complete node. Every 2016 blocks, all nodes will adjust the difficulty value according to the unified formula. This formula is obtained by comparing the spending time of the latest 2016 blocks with the expected time. The expected time is 20160 minutes, which is the total time calculated according to the generation rate of a block in every 10 minutes. According to the ratio of the actual time to the expected time, the difficulty will be adjusted.

Compared with Hashcash, bitcoin uses the SHA-256 algorithm. In bitcoin network, the first 32 bits of hash value should be zeros, and then the bitcoin network will periodically reset the difficulty to face with the increasing computing power of miners.

3) Application of POW in Bitcoin

In the bitcoin white paper, Satoshi Nakamoto proposed the application of POW in bitcoin network[1]. He described the following six points:

- New transactions are broadcast to all nodes.
- Each node collects new transactions into a block.
- Each node works on finding a difficult proof-of-work for its block.
- When a node finds a proof-of-work, it broadcasts the block to all nodes.
- Nodes accept the block only if all transactions in it are valid and not already spent.
- Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

In bitcoin network, to realize the process of POW, we should first generate Merkle root hash through Merkle tree algorithm.The figure2 shows transactions hashed in a Merkle Tree. After that, we judge whether 2016 blocks have been generated after the last difficulty value adjustment. If the condition is satisfied, the algorithm will adjust the difficulty. If the condition is not satisfied, we take the 80B data of the current block header, prev-block hash, bits, nonce, Merkle root, and timestamp as the input values of the POW. Furthermore, we continuously adjust the nonce, and perform double SHA-256 operation on the block header after each adjustment. Finally we compare the calculated value with the current difficulty value D. If it is less than the difficulty value, the mining is successful.

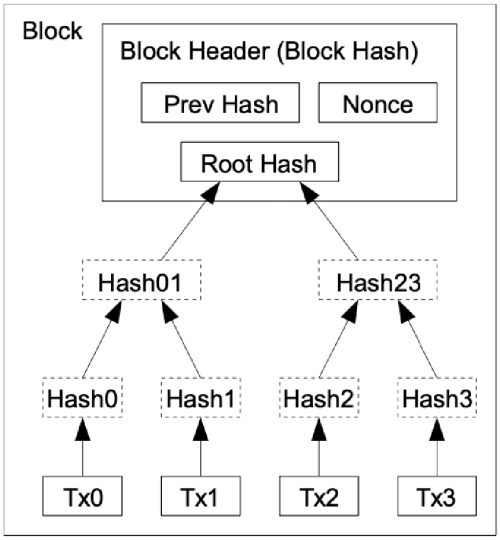

Fig. 2. Transactions hashed in a Merkle Tree[1]

4) Three Issues of POW

a) The Centralization of Computing Power

The proof of work(POW) of bitcoin is computationally intensive, which is easy to lead to the centralization of network computing power. In the bitcoin white paper[1], Satoshi Nakamoto proposed the concept of "one CPU one vote". In Nakamoto's vision, nodes can use personal computers to perform POW operations, participate in block node elections, and receive corresponding compensation. However, with the rise of bitcoin price, the block reward has attracted a large number of computing power to join, and the hash computing power in bitcoin network shows an exponential growth trend. The physical equipment of the consensus node participating in POW computing has been transformed from the early personal computer to GPU, and then evolved into the ASIC miner widely used at present.

In view of the computationally intensive characteristics of SHA-256 hash function, some blockchain systems choose to replace the original function with memory intensive hash function. For example, Litecoin and Dogecoin adopt the script algorithm, Ethereum adopts the Ethash algorithm, and

Zerocash and Zerocoin adopt the Equihash algorithm. Memory intensive hash function can reduce the computing power advantage of ASIC mining machine to a certain extent because it occupies a lot of memory and is difficult to compute in parallel.

b) Waste of Resources

POW of Bitcoin will lead to the waste of computing resources. The existing literature estimates that the annual power consumption of bitcoin network is equivalent to that of Ireland or Austria.

In order to solve the problem of resource waste, some blockchain systems use the computing power consumed in POW computing to provide useful services. For example, primecoin improved the pow problem to find prime numbers that meet the requirements, thus promoting the development of the field of mathematics.

c) Performance

Since the average block interval of bitcoin system is 10min and the block size is limited to 1MB, theoretically, the transaction throughput is about 7 transactions per second. Low throughput limits the wide application of bitcoin system. With the increasing attention of bitcoin system, the number of unconfirmed transactions in the network increases. As of July 10, 2019, there were nearly 50000 unconfirmed transactions on bitcoin network. The performance problem has become an urgent problem to be solved in bitcoin pow.

In view of the low performance of bitcoin pow, some research work and blockchain system improve efficiency by modifying parameters and improving block node election mechanism. For example, Ethereum, Wright coin and dogcoin systems adjust the block interval in the bitcoin POW mechanism to 15s, 2.5min and 1min respectively, so as to accelerate the transaction processing speed. Shortening block spacing seems to be a feasible scheme to improve performance. However, some research work has found that shortening block interval has potential security risks.

B. Proof of Stake

1) Proposal of POS

POW consensus algorithm submits a result which is difficult to calculate but easy to verify through the compute power competition among all nodes. Every node can verify the result through simple operation, so as to recognize the work of the verifier. This mechanism effectively maintains the security of bitcoin system. However, the unfair computing power, waste of resources, and low efficiency of POW algorithm seriously limit the expansion of bitcoin blockchain technology.

In view of the waste of resources in the POW, the bitcoin community proposed proof of stake(POS) in 2011 for the first time. The algorithm stipulates that the number of bitcoins owned by nodes is used to replace the process of solving hash value based on computing power in POW. The more bitcoins owned by miners, the greater the possibility of mining. The security of the POS mechanism is based on the fact that equity owners are more motivated than miners to maintain network security[1]. If the blockchain system is attacked, the interests of equity owners will be more likely to be damaged. In 2012, the proof of stake mechanism was applied in peercoin system for the first time.

2) Proposal and Concept of Coin-days

In the application of blockchain, it is impossible for us to truly allocate shares to nodes in the chain. Instead, other things are used as shares, and we allocate these things to nodes in the chain.

In the application of POS, the amount of currencies can be recorded as the number of equity. Now Ethereum has the POS consensus mechanism. Therefore, in Ethereum, the number of shares of each Ethereum node is measured by the number of Ethers. For example, in an Ethereum network with three nodes, A, B and C, A has 100 Ethers, B and C have 10 and 20 respectively, and then A block is the most likely one to be selected.

3) Concept of POS

Given a difficulty value D of the whole network and the trade data newly packaged into the block, the qualified counter can be found, as presented as Formula 2:

$$\mathrm{SHA256}\big(\mathrm{SHA256}(\mathrm{tradeDate}||\mathrm{Counter})\big) < \mathrm{D} \times \mathrm{Coindays} \quad (2)$$

The accounting rules of the POS consensus algorithm are basically similar to the POW consensus algorithm, while the POS consensus algorithm does not require miners to enumerate all the random numbers nonce, but only allows one hash value within 1s, which greatly reduces the computational work and curb the resource consumption in computing power competition.

4) Application of POS

Peercoin takes the Coin-ages as the equity to elect block nodes. The concept of Coin-ages is also applied in Cloakcoin and Novacoin. It can suppose that user A has 10 coins and holds them for 90 days, with a cumulative Coin-ages of 900. User B has 10 coins and holds them for 45 days, with a cumulative Coin-days of 450. According to concept of POS, user A is twice as likely to solve the problem as user B.

In 2014, Pavel Vasin proposed POS2.0 and applied it to blackcoin, so that the Black Coin developed from POW + POS consensus mode to pure POS consensus mode at that time. The rights equity in the POS2.0 consensus algorithm are directly proportional to the user's online time. This incentive mechanism effectively enhances the blockchain P2P network, prevents the occurrence of "tragedy of the commons" in the pow consensus algorithm, and greatly increases the difficulty for attackers to realize "51% attacks". However, POS is prone to bifurcation, and the decentralization of blockchain is weakened.

5) Nothing-at-stake Attack

Nothing at stake attack refers to the problem that the selected out of block node generates multiple blocks at the same height, resulting in block fork. As shown in Figure 3, the blockchain system based on the proof of stake forks at height h, and node A is the block out node at height H + 1. Since the block finally confirmed at height h is not determined, node A selects to generate blocks after the multiple forked blocks at the same time. Therefore, no matter which block is legal in the end, node A can make a profit.

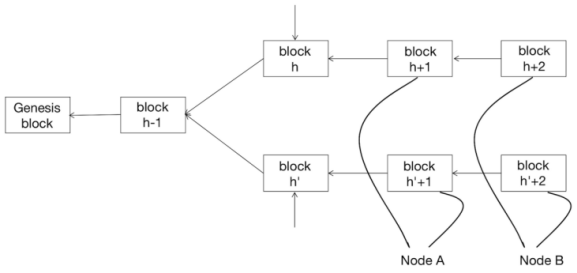

Fig. 3. Nothing-at-stake attack

The attack cost of nothing-at-stake attack is low, and the out of block node can generate multiple blocks without any cost. Therefore, the multiple forked blocks go hand in hand and never reach a consensus. The existing solutions to non equity attacks mainly include margin system and security hardware. Margin system means that the consensus node needs to deposit and withdraw a certain amount of margin in the account. If the node is monitored to launch a nothing-at-stake attack, its margin will be confiscated to solve the nothing-at-stake attack from the perspective of economic incentive. For example, both slasher and Casper of Ethereum's POS proposal have introduced the margin system. Similarly, Tendermint introduced a margin mechanism.

III. Conclusion

Blockchain technology is accelerating the development of digital economy in the process of integration with real industries. As the core technology of blockchain, the consensus algorithm can achieve the consistency of results on a specific transaction in a network environment where nodes are highly dispersed and there is no mutual trust mechanism, and there is no disagreement on the process and results. Generally, the choice of consensus algorithm is to balance efficiency, security and stability on the premise of specific application scenarios.

This paper focuses on the two aspects of POW and POS in the blockchain consensus mechanism, and analyzes the advantages and the existing problems of the two consensus mechanisms. Some typical algorithms are discussed in detail in this paper. Based on the current research status, in view of the development of blockchain consensus algorithm, it is necessary to study and solve the problems of performance and security. This paper is a great references for the researches studying on blockchain consensus.

References

[1] S.Nakamoto, (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.

[2] J.Bonneau, A.Miller, J.Clark, A.Narayanan, J. A.Kroll, & E. W. Felten,(2015, May). Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In 2015 IEEE symposium on security and privacy (pp. 104-121). IEEE.

[3] A. Back, (2002). Hashcash-a denial of service counter-measure.

[4] M.Jakobsson, &A. Juels, (1999). Proofs of work and bread pudding protocols. In Secure information networks (pp. 258-272). Springer, Boston, MA.

[5] A.Wahab,& W. Mehmood,(2018). Survey of consensus protocols. arXiv preprint arXiv:1810.03357.