Analysis of POW in Bitcoin and POS in Peercoin

Yihua Yu *

Faculty of computing, Harbin Institute of Technology, Harbin, China

* Corresponding author email: 120l021602@stu.hit.edu.cn

Abstract. The technology of blockchain, which is the underlying technology of cryptocurrency like Bitcoin, has changed the world dramatically and it has fascinated researchers from all over the world. Originating from the Byzantine General Problem, the consensus mechanism is utilized to reach an agreement in a group where the channel for communication could be unreliable. Among all the consensus mechanisms in the blockchain, proof of stake (POS) and proof of work (POW) are the most widely used. POW was first used in the Bitcoin blockchain and soon became its central consensus mechanism of it and the earliest implementation of POS for cryptocurrency was Peercoin. Numerous research has been done in this field, but they failed to explain the features of the two mechanisms comprehensively. In this paper, the author did a brief introduction to the hash function and consensus mechanism as well as how POW and POS work, then made detailed analysis and comparisons of a POW in Bitcoin and POS in Peercoin in terms of fairness, security, environmental influence, penalty, negotiability and sustainability, and future trend, and declared that both of POS and POS had some advantages and drawbacks. The author also listed some risks and potential problems of POW and POS and then gave possible solutions for them.

Keywords: Consensus Mechanism; Proof of Work; Proof of Stake; Bitcoin; Peercoin.

1. Introduction

The concept of blockchain was firstly proposed by Satoshi Nakamoto in 2008[1]. The blockchain technology was initially used in Bitcoin and because of its superiority, it has developed rapidly in recent years. Nowadays, besides cryptocurrency, the technology of blockchain is employed in various fields such as finance, insurance, Internet of Things and logistics, public management and so on [2]. The blockchain has the feature of decentralized. A decentralized network signifies that each node is independent and there is no central system to control the whole network, which is totally different from the traditional centralized network structure where all the data and process have to rely on a single entity (like server and data center) [3]. However, it is difficult to achieve unanimous approval about the information spread on the distributed network. Consensus mechanism were designed to deal with it. Consensus mechanism has its roots in Byzantine General Problem (BGP)[4]. It describes a situation that a group of generals were attempting to reach an agreement to either attack or retreat. But there were some betrayers among these generals who could send erroneous messages, which might affect the loyal generals to act oppositely. So, a consensus mechanism is needed. In the distributed computer network, there are malicious nodes, like hacker nodes which can do harm to the Internet, so it is essential to establish a consensus mechanism to make sure that all the honest parties on the Internet make an agreement of the transactions. A lot of research has been carried out and there are more than 30 consensus mechanism of blockchain, among which POW and POS are the most popular ones. The fundamental difference between this consensus mechanism is which node adds a new node to the blockchain. In 2008 Satoshi Nakamoto introduced the mechanism of POW to the public and created a great sensation [5]. Sunny King published Peercoin and firstly announced the use of POS for cryptocurrency in 2012. Then came the delegated proof of stake (DPOS) of Ethereum in 2014[6]. Scientists have been working on the combination of POS and POW of Ethereum. Having a full understanding of POW and POS is of critical significance to make further contributions to the blockchain consensus mechanism. Nonetheless, former research failed to compare POW and POS comprehensively. In this paper, the author compared POW in Bitcoin and POS in Peercoin in six aspects: fairness, security, environmental consumption, penalty, negotiability and sustainability, and future trend, and elaborated the features of POW and POS in detail. The author declared that both of

POW and POS had advantages and flaws. The author also analyzed some risks that could damage the stability of POW and POS and gave some possible solutions for them.

2. Preliminary

2.1 Hash Algorithm

Hash algorithm is used universally in cryptography as well as blockchain. A hash algorithm has three main characteristics [7]. Firstly, a hash algorithm accepts arbitrary strings and the length of the output is always the same no matter what the length of the input is. Secondly, a hash algorithm is collision-resistant, which means it is impossible for people to find two different input that leads to the same output. Thirdly, the complexity of computing the hashing value of input x (a string with length of n) is O(n), which implies the hashing value of a particular string can be computed in a reasonable amount of time. In Bitcoin blockchain, POW mechanism uses a secure hash algorithm called SHA256 which was designed by National Security Agency (NSA) [8]. The output of SHA256 is 256 bits. As it was elaborately-designed, changing one bit of the input would lead to an extremely different output.

2.2 POW

POW is the oldest and most widely used consensus algorithm. The idea of POW is that the consensus is based on the computing work that nodes have done. The creation of a block is associated with a difficult math problem and the node which solves the problem can add a block to the blockchain. In Bitcoin, transactions are broadcast to the public and each node on the Internet collects these transactions into a block of their own. A Bitcoin block contains three components: previous hash, nonce and transactions [9]. In the POW mechanism in Bitcoin blockchain, the hard math problem is finding the SHA256 hashing value which starts with a number of zero bits by exhaustively searching the nonce. The nodes are called miners and the computing process is called mining. Computing the hashing value requires a great amount of computing power and once the hashing value is calculated, the corresponding miner add a new block to the blockchain with its wrapped transactions. As a reward, a node receives some Bitcoins. Then the miner broadcasts its hashing value to the network. So other miners will know the previous hashing problem has been solved and start new mining process. If there are forks in the blockchain, the fork with the longest chain wins and all transactions in the other chain is considered invalid.

2.3 POS

POS is firstly used in Peercoin and it has become the second popular consensus mechanism worldwide [10]. In the POS system, the consensus relies on the stake of each node. The unit of POS in Peercoin is coin-day, namely the amount of money multiplies the time it has been held. Each node on the peer-to-peer network is called validators and the possibility of a node to be selected to add its block to the chain is identical to its portion of fortune over the network. In other words, the more coin-day a validator has, the more likely it is chosen to create a new block. In order to create a new block, a chosen validator needs two inputs: kernel input and stake input. Kernel input is an input which leads to a certain hash target. While stake input is the coin-days the validator has to spend to create a block and the more coin-days a validator spends, the quicker the hashing process. The new block contains the transactions collected by the validator. In POS in Peercoin, the computing of hashing is a lot easier than POW in Bitcoin because the input is searched in a limited space rather than an unlimited search space.

3. Analysis and Comparison

Both the POW and POS are fair. In Bitcoin blockchain, each node which owns computing power can become a miner and contribute to guarantee the justice of POW of the public chain. The more

effort a miner has done, the better reward it will get. Which means the Bitcoin award for a miner is proportional to the computing effort it has done. In Peercoin POS mechanism, each node owns non-zero coin-days can join the process of validation and the rate of being chosen to generate a new block is proportional to the stakes(coin-days) it holds.

In the blockchain of Bitcoin, a fork of the chain occurs when two miners solve the hashing problem simultaneously. Malicious miner on the network can make use of the fork to conduct attack. One classic attack is "Double spend attack", which means A uses the same Bitcoin to make deal with B and C at the same time and the two transactions are written in two forks. In Bitcoin blockchain, this kind of attack is effectively avoided. In fact, the possibility of two miners mining blocks at the same time is rather low and the possibility of two forks with the same height of two is even lower. When a fork is longer than another, the honest party has to switch to the longest chain and the blocks on the shorter chain are abandoned. The transactions in a block are not considered valid until there are six blocks added to the block. It is secure because after six blocks, the possibility of the existence of another fork is negligible. "51%attack" threatens the security of Bitcoin blockchain. If a miner owns 51% of the computing power on the network, it is capable of making one fork the longest, and thereby add illegal transactions in the blocks. Suppose the total hashing power of the Internet is H, the hashing power of malicious miners is qH, and the hashing power of honest miners is pH($p+q<1$). q_z is the probability that an attacker ever catches up with the honest chain when the attacker's chain is z blocks behind. Equation (1) shows the malicious party can make the chain longest as long as $q>p$.

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases} \tag{1}$$

However, it is almost impossible for a miner to have over a half of the total computing power because the incredible high cost. Take Antminer S9 for example, if it wants to conduct 51%attack, the total cost for its hardware is 9,620,049,467 dollars (showed in Table 1).

Table 1. Cost of hardware of 51% attack

Computing power of one machine	price of one machine	51% target computing power	cost of the 51%attack(hardware)
14,000 GHash/s	2400 dollars	56,116,955,221 GHash/s	9620049467 dollars

As for POS in Peercoin, the blockchain is free from the forking process because only one validator is selected at one time to generate a new block to the chain, instead of all the nodes on the network joining the mining process together, which is a great advantage for Peercoin which means all the negative effects from forking disappear. Similar to 51%attack in Bitcoin, the POS blockchain in Peercoin is considered secure only if the honest party owns more stakes than the malicious party. However, the cost of owning 51% of all the stake may even be higher than the cost of 51%attack in Bitcoin so the probability of malicious party owning 51% of all the stake is negligible. Besides, the counterfeiting of Peercoin is extremely difficult, and the validator has to pay part of the stake to generate a new block and there are no transaction fees as reward, which raises the cost of attacking. Peercoin also has a centralized checking system to check whether the transactions in a block are valid, which helps to reinforce the security of the POS blockchain.

The POW does harm to the environment, while POS does not. In Bitcoin blockchain, miners all over the world compete to mine a new block and this competition is getting more and more intense. The cost of mining has now risen so that people cannot rely on household devices, like smart phones laptops to do the mining, instead they have to use some fancy equipment which consumes a lot of electricity. Up to May 10, 2021, the annual electricity consumption of global Bitcoin mining is approximately 149.37 terawatt hours. The great amount of electricity is produced from natural resources like fossil fuel and nuclear power and the process of generating electricity consumes

precious natural resources which is limited on earth and most importantly, causing great pollution to the environment. However, the Peercoin with POS mechanism does little damage to the environment as the hashing validators do is simple and quick. The consensus relies on the consumption of the stake rather than the consumption of electricity.

In Bitcoin blockchain, each miner can join and quit mining at any time and all the miners are anonymous. The POW mechanism does not have a penalty for malicious miners who conduct attack to the blockchain, which gives them little apprehension about being punished and space for future attack. But POS in Peercoin does have penalties for those malicious validators. If a validator is found by the checking system to forge invalid transactions in a block and add it to the blockchain, it will be deducted part of its coin-days as punishment. The negotiability of Bitcoin is better than Peercoin. As for Peercoin, a validator gets coins based on its holdings. If a validator spends some coins to make deal with another validator, its total coin-days declines and the probability of being selected to mint a new block also declines. So, from psychological view, a validator prefers holding the coins to spending them. However, the right to generate a new block has nothing to do with the coins miners keep, so it is more acceptable for a miner to spend its coins, thus accelerating the negotiation of Bitcoins.

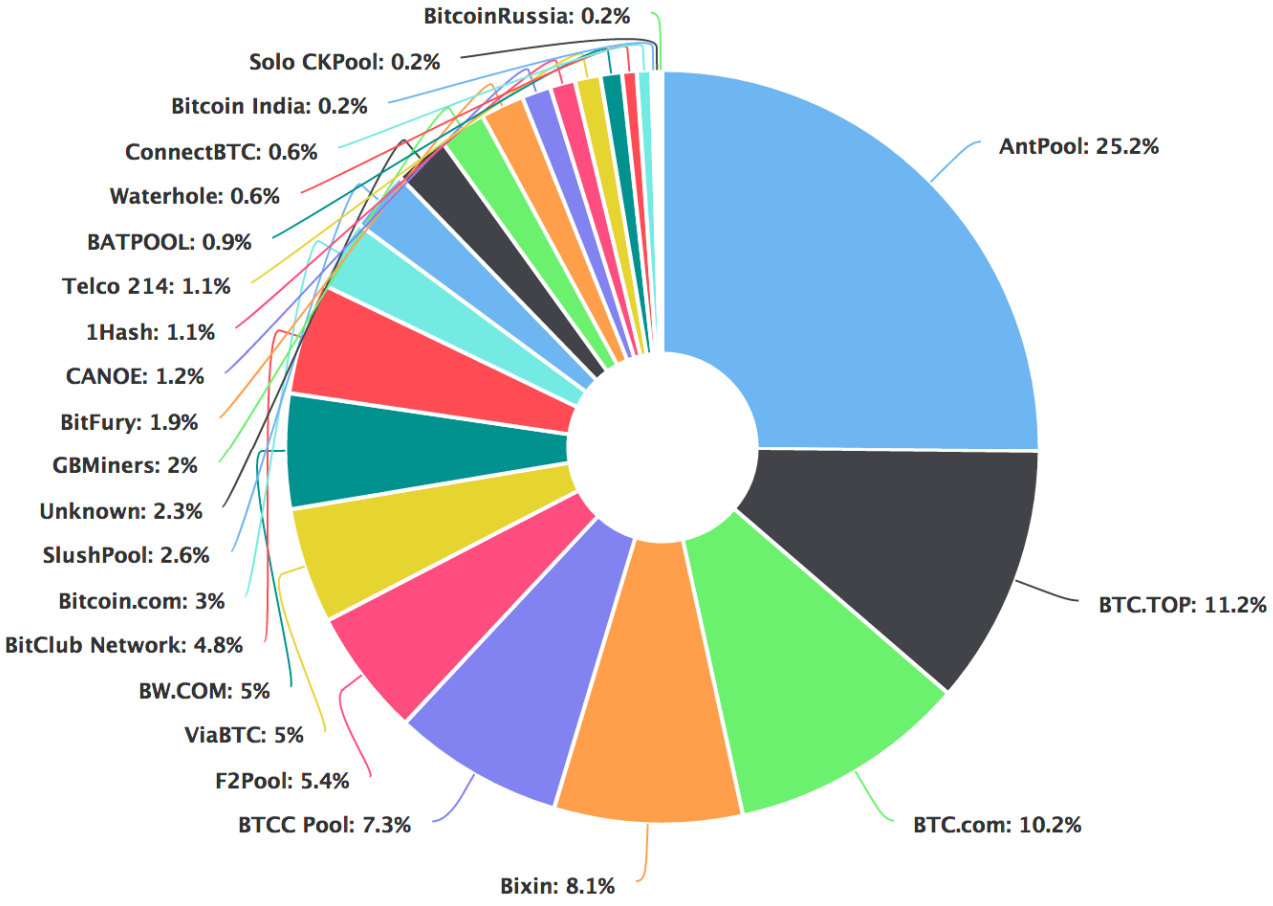


Fig 1. Ratios of mining pools

POW in Bitcoin and POS in Peercoin are developing with a spectacular speed, but there are some risks and concerns about them. Fig shows the distribution of the mining pools in the world. Although none of the pools owns 51% computing power, if the top three mining pools work together, they are able to conduct 51% attack. Also, the power and finance of a government is strong enough to conduct 51% attack. If Bitcoin is interfered with constitution of level of government, it will be destroyed entirely. Another risk of Bitcoin blockchain is the sustainability. As mining is becoming harder, there fewer people bother to dedicate the effort and time, and thereby the number of nodes on the network

decreases. As a result, most computing power is gathered in the hands of a few people, which makes the blockchain more centralized and restrains the growth of Bitcoin blockchain. The sustainability is also a serious issue for Peercoin because it also favors the rich. The rich are likely to become richer so that it is possible that there will be no room for the poor one day. Another risk of Peercoin blockchain is that a chosen validator does not turn up to do its job (mint a new block and validate transactions). It can be quite serious because if it happens, the whole blockchain will be stagnating. A possible solution for it is choosing some nodes as back-up validators in case the situation occurs.

4. Conclusion

Consensus mechanism is the core of blockchain and POW and POS are the two most widely-used consensus mechanism which attract researchers around the world. In this paper, the author introduced two specific implementations of POW and POS, which is Bitcoin and Peercoin, and then analyzed and compared the fairness, security, environmental influence, negotiability, sustainability of POW and POS. The author found that both two mechanisms are fair and secure, but only POS is environmental-friendly and in good design of penalty system, and the negotiability of POW is better than POS, and POW and POS all have the problem of sustainability. The author used accurate descriptions and made comprehensive comparisons to show the features of POW and POS, which helps researcher to fully understand the two-consensus mechanism and carry out further research. As there is no penalty in Bitcoin blockchain, research is needed to introduce a proper penalty system into Bitcoin. And for both POS and POW mechanism, attention needs to be paid to the sustainability of cryptocurrencies. Only if these potential problems be solved can the technology of blockchain have a bright future.

References

[1] Lamport L, Shostak R, Pease M. The Byzantine general's problem[M]//Concurrency: the works of leslie lamport. 2019: 203-226.

[2] Zheng Z, Xie S, Dai H N, et al. Blockchain challenges and opportunities: A survey[J]. International journal of web and grid services, 2018, 14(4): 352-375.

[3] Zhu X, Zhang Y, Zhao Z, et al. Radio frequency sensing based environmental monitoring technology [C]// Fourth International Workshop on Pattern Recognition. SPIE, 2019, 11198: 187-191.

[4] Song H, Zhu N, Xue R, et al. Proof-of-Contribution consensus mechanism for blockchain and its application in intellectual property protection[J]. Information Processing & Management, 2021, 58(3): 102507.

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

[6] King S, Nadal S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake[J]. self-published paper, August, 2012, 19(1).

[7] Merkle R C. A fast software one-way hash function[J]. Journal of Cryptology, 1990, 3(1): 43-58.

[8] Kammoun M, Elleuchi M, Abid M, et al. FPGA-based implementation of the SHA-256 hash algorithm [C]// 2020 IEEE international conference on design & test of integrated micro & nano-systems (DTS). IEEE, 2020: 1-6.

[9] Underwood S. Blockchain beyond bitcoin[J]. Communications of the ACM, 2016, 59(11): 15-17.

[10] Wan S, Li M, Liu G, et al. Recent advances in consensus protocols for blockchain: a survey[J]. Wireless networks, 2020, 26(8): 5579-5593.