Analysis of consensus mechanisms: PoW and PoS

Jiang Wenxuan

Ningbo Xiaoshi High School, Ningbo, Zhejiang, China, 315000

vincentjiang0207@163.com

Abstract. Along with the trend of Bitcoin blockchain, the concept behind all virtual currency has become popular in the study of the Internet. This essay mainly researches two kinds of common consensus mechanisms for the current blockchain network and looks forward to the future development of the technology's usage in daily life. This research aims to overview the two most common consensus mechanisms in the construction of blockchain. By reviewing resources from other research, an explanation of the goal of the consensus method, the advantages, and disadvantages of each approach and the future development of these two methods are summarized and developed. The result of the review explains the shifts of mature virtual currencies from proof of work to proof of stake and advises what mechanism should be used at starting stage and why a shift is necessary for proof of stake currencies.

Keywords: PoW, PoS, consensus mechanism, blockchain, virtual currency.

1. Introduction

Just like what Satoshi Nakamoto said in his paper, "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution" [1]. Bitcoin is a kind of electronic cash in which there is no trusted third party required. As a kind of currency which is going to lead the world's development in the future, the importance of researching and overviewing the current mechanism development is significant.

In detail, this paper focused on the advantages and disadvantages of proof of work and proof of stake, known as PoW and PoS. The review of the structure of the algorithm and document from the developers is the source used by this report. By summarizing the feature of the two methods, both the long-term and short-term influences are discussed, and risks of exchanges and starting stages' problems are also evaluated in the paper. The method of research is by overview mechanism of both proves and summarize their features. Furthermore, the situation is stimulated to evaluate the advantages and disadvantages of a specific currency development or usage stage.

As a strong foundation, the report, which is a consensus mechanism analysis, could help researchers or organizations to make a better choice when constructing their new currency in the future. It would help other resources to summarize the new mechanism's advantages and disadvantages.

2. Basic knowledge of blockchain and consensus mechanism

Blockchain is a chain list which connects blocks. In each block, numerous things are packaged, such as all trade data and a new key for the next block. The most important feature of a chain list is a connection to the next block requires addressing information in the block, and thus the problem of double pay and modification of the contents of the block easily. The original blockchain is invented by Satoshi Nakamoto, and the product of this algorithm is Bitcoin, known as BTC. A schematic diagram for the original blockchain is shown in figure 1. In this schematic diagram, the inheritance of the blockchain is displayed, which is the connection between the first transaction and the following transaction that needs the previous key to verify the signature.

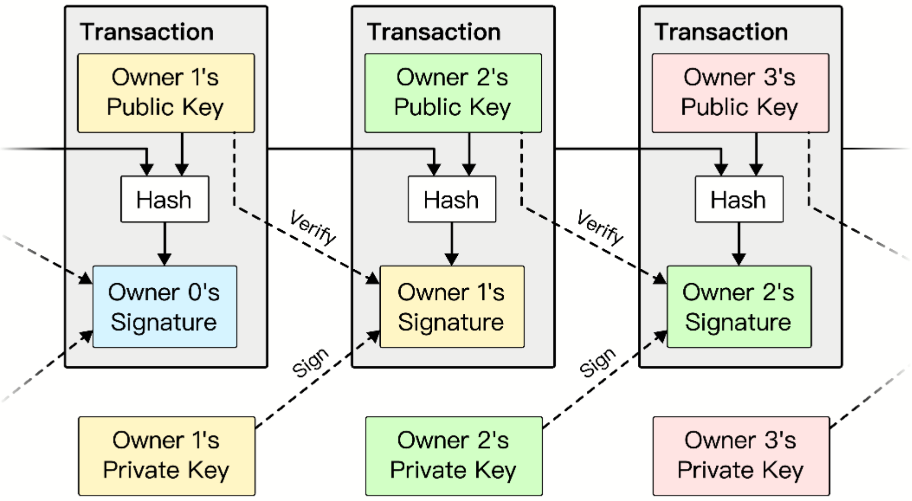

Figure 1. Schematic diagram of blockchain [1].

The idea of blockchain is essential for a currency without a third party. It provides the currency with numerous features different feature. However, the concern remains. In this paper, how to make a new block is the focus, and different consensus mechanisms would be researched. “Blockchain technology, the consensus mechanism determines the security, scalability, and decentralization of Blockchain” [2].

As the mechanism is introduced, the production of a new block is not defined properly. If a new block would be produced easily, too many branches of a blockchain would destroy the currency since people do not know where to write their trade and no branch would be really overall. Tons of merge processes are required and always required.

Blockchain has many outstanding features, such as immutability, security, speed, and consensus as Lashkari mentioned in his review, and the consensus mechanism is the source of this feature [3]. For the consensus mechanism, the main idea is to add some obstacles for creating a new block and the difficulty would be verified easily. As the description shows, a one-way function is required for this obstacle. With this mechanism, the block produced would be much more reasonable and more people would trade on it and tend to add a new block after it, which is also known as consensus.

Furthermore, a different way of proof would be possible if the current owner does not only determine the validity by the computer power. Another kind of consensus mechanism is based on the stake (currency) that the block creator owes and the standard of creating a new block is the currency they held (often, the time of holding is also considered an important factor).

3. Proof of work

For the proof of work, the main idea of this mechanism is to set a difficult task which would be difficult for everyone in every block, and thus it is difficult to add a new block. Two widely used approaches of proof of work are one-way function and space-time exam.

3.1. Hash applied to bitcoin

For the hash, the most widely known example is bitcoin. It is the basis of countless different currencies. Bitcoin creates a fundament for all other algorithms using the hash. Although other, more practical ways have been developed, it is still critical for us to learn how a simple hash function works for blockchain.

The main idea is to find a difficult problem and start to modify it. In this case, using the hash function secure hash algorithm 256-bit, to produce a number with numerous zeros at the first of the answer. This issue is relatively random, and no trend could be obtained. So, a huge number of trials, which means computing power, is required to make a new block. When the zero number increases, the difficulty of the concern increases as well. The change in difficulties would help to limit the rate of block produced.

However, solving a problem would not avoid the modification concern, so the real rule of new block development is based on the data in the previous block. Every time when the miner wanted to produce a new block, their hash value needs to be added with the previous value of all the trades in the block, the signature of the miner who make the last block and the last block's hash. If someone would like to modify the previous trade records, these people need to redo the hash calculation. Moreover, changing the content in the block means the miner must change all the following blocks.

Using this kind of algorithm, the blockchain would be produced. Choosing bitcoin as an example is great since its process is easy to understand and straightforward. In other cases, some currencies would use a different hash function or a different way of validation, and some coins even use MD5 message-digest algorithm as their one-way function (it has been proven to be easy to crash). This algorithm would be the mode widely known approach.

3.2. Storage applied for proof of the capacity

POC means proof of capacity. It is different from the hash approach mentioned above. The examination takes place by storage ability. The developer of this mechanism claims it would not cost a lot of power compared to bitcoin. However, the end of POC causes a gigantic rise in hard disk prices.

Most of the POC would also include time as another factor. Every time when a miner claim they have this ability of storage, the examiner request would be sent, and the miner needs to rent the request. A verifier can check if a prover has stored the data they committed to over space and over a period.

3.3. Advantages of proof of work

The advantages of PoW are that it is a strong verification for every people, and it could be used at the start phase of a currency. Everyone would verify easily because it relied solely on a one-way function or simple same message. A hash function would be difficult to obtain a certain value, but easy to calculate a value.

Moreover, in the process of building blocks, the total amount of currency is not enough at first. The consensus mechanism cannot be based on stake. For the PoW, it would reward the first group of miners with some currencies. It would encourage them to build this blockchain more and get more rewards due to the increase in the value of coins. No matter what time it is, the PoW mechanism would be useful for building blocks, since it depends solely on solving problems, instead of proving a huge amount of currency owned. Furthermore, this method of construction of new blocks could prevent forking because of limited computing power for every miner. As explained by Cointelegraph, "A miner would have to split their computational resources between the two sides of the fork in order to support both blockchains. As a result, through an economic incentive, proof-of-work systems naturally prevent constant forking and urge the miners to pick the side that does not wish to harm the network" [5].

3.4. Disadvantages of proof of work

As the currency developed more, plenty of disadvantages appear. When the difficulties of producing a new block increase to a high level, a huge number of resources, such as computers and electricity, would be wasted for calculating a simple hash function. And as the currency developed, even more resources would be required. According to Bonheur, "Powerful computers inherently consume a lot of energy. Furthermore, these machines require effective heat management or cooling system to remain operational and prevent overheating, as well as associated damages to hardware components due to internal heat build-up" [6].

Moreover, when someone wants to attack a kind of currency, a 51% attack is possible for some currency at the start. Since not plenty of miners are focusing on this blockchain, the attackers would use

51% of their computing power to create a whole new branch and replace the original chain. It is possible to happen if someone really aimed to attack. So, it would increase the probability of being attacked by excessive computing power.

4. Proof of stake

The basic concept of proof of stake is that instead of using computer power as the indicator of the capability to build a new block, PoS is aiming for using a stake to prove the validity of a new block. In this way, relatively less computing power is required to maintain a currency and more problems emerge.

4.1. Ethereum 2.0

It is widely known that Ethereum, known as ETH, is another widely used currency which uses PoW to create new blocks on the blockchain. However, in the next version of the ETH, its developer decided to shift to PoS. Before this transition, a huge amount of energy usage is required for bitcoin mining and ETH mining. For the further development of this currency, a shift is needed.

For ETH 2.0, PoS has been used. In principle, PoS is a new consensus mechanism for ETH which "This staked ETH then acts as collateral that can be destroyed if the validator behaves dishonestly or lazily. The validator is then responsible for checking that new blocks propagated over the network are valid and occasionally creating and propagating new blocks themselves" [4]. As the schematic diagram in figure 2 shown, a part of the stake of the block creator would be used to verify the new block's validity, and the stake decision chooses whether it would be the main branch or not to be selected.

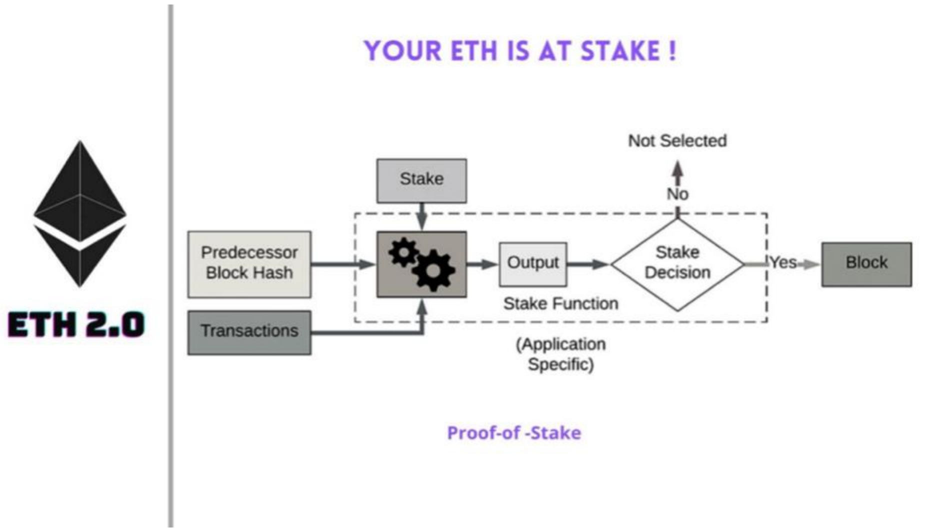

Figure 2. Schematic diagram of PoS used by ETH 2.0 [4].

It asks a group of validators to deposit some ETH into a contract and run software programs. The validator is responsible for creating a new block and sending it out to other people in the network. Furthermore, a feature of finality is introduced, which means the block's content cannot be changed unless a lot of ETHs are burnt. Only two-thirds of the people agree the process would take place.

4.2. Advantages

PoS mechanism only requires currency to prove the stakeholder's ability to maintain a block, instead of using plenty of resources to verify their ability. In most cases, the PoS chain of a currency is developing a lot faster than the PoW chain, and thus, the speed of payment is faster. According to Gehmlich, "The proof-of-stake solves scalability issues that have been a thorn in the flesh in the proof-of-work consensus mechanism. PoS facilitates faster transactions since blocks are approved faster as there's no need to solve complex mathematical equations. Since no physical machines or mining farms requiring ample energy supplies are needed to generate consensus, there is better scalability" [7].

For another reason, the people who take part in PoS are more likely to contribute more to the currency. Because they hold a lot of this kind of currency, improving in value of these coins would be beneficial for them, which means they want to and would work on it. For them, they have a good reason to maintain a new block nicely and fast. It is essential to reward the people who want to improve this currency. For the PoW, some miners might just complete the work and sell the coins.

Moreover, it is less likely that a coin-used PoS would experience a 51% attack. Since it is possible that the attacker uses a lot of computer power to attack a coin, the 51% attack for a coin based on PoW is possible when it is relative, not popular. However, no matter what kind of coin, it is much more difficult for an attacker to control 51% of the coin. In some algorithms, change blocks even require the attacker to have two-thirds of the total currency. It is much more difficult and if you really have that number of coins, the people will not want to attack.

4.3. Disadvantages

One of the disadvantages is that in a normal PoS community, more stake means more power in policy-making, but that is not always the case. It is usual for more people to invest some of their money into electric currency such as bitcoin and ETH, but they would not create their own electric wallet. Instead, they would only open an account on a platform and the platform would help them purchase and sell all the coins. For the concept of stake equal to power, people who owe the coins do not have the right to vote since the platform helps them to keep them, which means some massive cooperation might make several bad decisions to make these coins bad. And it is also difficult for most people to understand and try to use a hash code as their account.

In another case, if the coins just start developing, PoS is not likely to work. Not numerous people have coins, and they could only buy them from other people or from mining. It is possible that only the introducer of the coin would maintain the chain and the reward cannot be distributed thus the influence of the coins cannot increase. As a result, no one would spend more on this coin. So, it is inappropriate to use PoS at the beginning of a new electric currency.

Furthermore, proof of stake might cause the problem of centralization again. According to Chandler [8], since there is no limit on how much crypto a single validator could stake, a huge validator might act like a bank and control the currency.

5. Future development of consensus mechanisms

Nowadays, more and more consensus mechanisms are being developed. Combined networks such as "an improved network for blockchain is proposed to combine different blockchain networks together. It uses the POU consensus mechanism to improve the network environment, which consists of Proof of Stake Entrance, Hash Net Verification and Delegated Parliament" [9]. This kind of mixed network requires a different level of explaining and evaluating since it would combine the effects, too. Moreover, different methods from basic are developed, such as Proof-of-Stake with Delegated Ownership (DPoS) Blockchain-based Consensus and Fault Tolerance in the Byzantine Style (BFT) [10].

In the future, blockchain and electric currency will be used more and more. Furthermore, the certain difference would appear while developing. The content in each block would increase and the frequency of requests and receive would increase noticeably. To cope with this increase in demand for trade, better algorithms would be developed and applied to the currencies. Moreover, the ability to be updated is also being considered. Instead of having a different currency, a future developer should be able to update existing currency and blockchain. It could reduce the cost of transfer a lot. In the future, the blockchain could be used for smart contracts and create a global country. It is possible to see that during the usage of the electric currency, the concept of country and world could change. In mete verse, more currency system needs to be established. Moreover, NTF has appeared for a long time, and this merchandise could be stored on a blockchain. The more the title represents all kinds of possibilities.

6. Conclusion

In conclusion, the features of the PoW and PoS are varying, and all comes down to a simple fact: PoW is better for starting and PoS could be used for further development. It is certain that PoS will be the mainstream of blockchain in the future, but the contribution of the PoW should not be forgotten.

The lack of method analysis is one of the improvements that the report could improve. Moreover, practical examples of risk for PoW and PoS could be added to illustrate these advantages and disadvantages in much more clarity and detail. These improvements could help readers to think about the current virtual currency's development and provide important resources for them to make choices in the mechanism's use.

References

[1] Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto Institute. (n.d.). Retrieved March 7, 2023, from https://nakamotoinstitute.org/bitcoin/

[2] Liu, Z., Liu, W., Zhang, Y., Xu, G., & Yu, H. 2019. Overview of Blockchain Consensus Mechanisms. *Journal of Cryptologic Research*, **6**, 395–432. https://doi.org/10.13868/j.cnki.jcr.000311

[3] Lashkari, B., & Musilek, P. 2021. A Comprehensive Review of Blockchain Consensus Mechanisms. IEEE Access, 9, 43620–43652. https://doi.org/10.1109/ACCESS.2021.3065880

[4] Proof-of-stake (PoS). (n.d.). Ethereum.Org. Retrieved March 7, 2023, from https://ethereum.org

[5] Proof-of-stake vs. proof-of-work: Pros, cons, and differences explained. (n.d.). Cointelegraph. Retrieved March 12, 2023, from https://cointelegraph.com/blockchain-for-beginners/proof-of-stake-vs-proof-of-work:-differences-explained

[6] Bonheur, K. (2021, September 15). PoW: Advantages and Disadvantages of Proof-of-Work. Profolus. https://www.profolus.com/topics/pow-advantages-and-disadvantages-of-proof-of-work/

[7] Gehmlich, B. (2022, October 10). Pros and Cons of Proof of Stake for Ethereum Blockchain Security. Gigster. https://gigster.com/pros-and-cons-of-pos-for-ethereum-security/

[8] Chandler, S. (n.d.). Proof of stake vs. proof of work: Key differences between these methods of verifying cryptocurrency transactions. Business Insider. Retrieved March 12, 2023, from https://www.businessinsider.com/personal-finance/proof-of-stake-vs-proof-of-work

[9] Guo, H., Zheng, H., Xu, K., Kong, X., Liu, J., Liu, F., & Gai, K. 2018. An Improved Consensus Mechanism for Blockchain. In M. Qiu (Ed.), *Smart Blockchain* **11373**, 129–138. Springer International Publishing. https://doi.org/10.1007/978-3-030-05764-0_14

[10] Blockchain Consensus Algorithms: What and How? Blockchain Certification Programs CBCA. (n.d.). Retrieved March 7, 2023, from https://www.cbcamerica.org/blockchain-insights/blockchain-consensus-algorithms-what-and-how