Proceedings of the 2nd International Conference on Business and Policy Studies
DOI: 10.54254/2754-1169/12/20230624

Comparison on Proof of Work Versus Proof of Stake and Analysis on Why Ethereum Converted to Proof of Stake

Mingjie Chen[1,a,*]

[1]*Warren College, University of California San Diego, La Jolla, California, United States, 92093*
a. mic018@ucsd.edu
**corresponding author*

Abstract: As approaching the era of Ethereum 2.0, the already unique and innovative cryptocurrency will witness a game-changing upgrade, and in this context, there is a lively discussion of the Proof of Work (PoW) and Proof of Stake (PoS) consensus mechanism. Moving from a PoW consensus mechanism to a PoS consensus mechanism is one of the most anticipated changes in this update. A close comparison of the two most popular consensus mechanisms, PoW and PoS, provides some strengths and drawbacks to these mechanisms. This comparison then becomes the building block to identifying the reasons behind Ethereum's upgrade to Proof of Stake. With the help of the comparison, this paper identifies a few drawbacks of the PoW consensus mechanism that Ethereum is currently facing. This paper finds that Ethereum's shift to PoS has indeed reduced the drawbacks of the Proof of Work consensus mechanism, mainly in terms of energy consumption, transaction cost, and confirmation speed.

Keywords: proof of work, Proof of Stake, cryptocurrency, Ethereum, consensus mechanism

1. Introduction

Digital currency is a currency system based on mathematical encryption, with Bitcoin being the first ever digital currency. It uses blockchain technology to accomplish safety between different users. With the application of blockchain, it can make the entire ledger public to everyone. When discussing cryptocurrency, the idea of consensus mechanisms comes into play. Generally speaking, the consensus mechanism is to solve the so-called decentralized trust problem because each node is untrustworthy. Consensus mechanisms between all nodes ensure the accuracy and security of recorded information as much as possible. However, no consensus mechanism is perfect; each has its own advantages and disadvantages, and some consensus mechanisms are born to solve some specific problems. As Ethereum is upgrading to the PoS consensus mechanism in September 2022, it is essential to understand why they are converting to PoS from PoW since Bitcoin has kept the PoW consensus mechanism till now. Whereas Ethereum is the second largest cryptocurrency after Bitcoin in the world, they are taking this move to upgrade the consensus mechanism. In order to understand the reason behind Ethereum's change to Proof of Work, this paper will first have a close comparative analysis of the two consensus mechanisms being mentioned. Then, comparing the disadvantage of PoW and the advantage of PoS will lead to some conclusions on why Ethereum is converting to PoS. By finding the reason behind Ethereum and analyzing whether it is a wise move, other cryptocurrencies facing the same problem as Ethereum can choose a similar path.

DOI: 10.54254/2754-1169/12/20230624

2. Consensus Mechanism

2.1. Proof of Work

Proof of Work is a popular type of consensus mechanism in which one node proves to the other node that they spent computational power achieve solving problems [1]. The idea was invented by Moni Naor and Cynthia Dwork in 1993, and later used by Bitcoin as their consensus mechanism to prevent problems such as decentralization. This approach can maintain the ledger security.

Blockchain is an enormous database, and everyone has access to this. If only a few people use this ledger, they can quickly identify all the transactions and authorize new transactions to be recorded if all people agree. However, in real life, this ledger is shared with a vast number of people, and we will not trust strangers to get control of the ledger. This is when PoW gets into play; proof of work ensures that users are not allowed to pay for funds they do not have the right to use. The proof-of-work algorithm combines math theory and cryptography to allow everyone to update the blockchain according to the rules.

Blockchain is the ledger mentioned above; instead of adding transactions one by one, transactions are packing them into blocks. After publishing transactions on the network, the user who created the block then counts the transaction as a candidate block. The transaction is valid only if the candidate block becomes the confirmed block. The fees for adding blocks are not cheap. Proof of Work requires miners (users who create blocks) to use their resources to compete for adding the block. In this case, the resources are computing power(energy), which can be used to hash block data until a solution to the puzzle is found [2]. Hash block data refers to bringing the data into a hash function to generate a block hash value. The block hash is unique, and it is an identification of the input data. Miners can only bring the data into a hash function to verify that the conditions are met. If it does not match, the data is slightly modified, and a different hash value is obtained. Unfortunately, changing even one character in the data can produce very different results, so the output is not predictable at all. When other nodes confirmed the data is correct, the entire network can update their ledgers to incorporate new blocks.

2.2. Proof of Stake

The Proof-of-Stake algorithm was launched in 2011 to solve the 51% attack problems with Proof-of-Work [3]. Although the two algorithms share the same goal of achieving blockchain consensus, the process for achieving the goal is quite different. Participants do not need to provide proofs that require intensive computation, only that they have staked their tokens. Proof-of-stake algorithms random selections to select validators from a set of nodes. In proof of work, all new blocks are not being mined, it is defined as “forge” a new block. Users participating in the process must lock a certain number of tokens into the network as their stake, this is to prevent adversaries from taking over too many validations [4]. The size of the stake determines the chance of selecting a node as the next validator. The greater the stake, the greater the chance.

To ensure that the process is not only biased towards the richest nodes in the network, it implements several special ways to ensure some randomness. Some commonly used methods are "Randomized Block Selection" and "Coin Age Selection". In the random block selection method, validator selection is determined by finding the node with the lowest hash and highest stake combination. People can always try to predict the next validators due to the publicity of the ledger. The coin age selection method selects nodes according to the staking duration of the tokens. The coin age can be calculated by multiplying the number of days that tokens are held as equity multiplied by the number of pledged tokens [4]. When a node forges a block, its coin age is reset to zero, which helps prevent nodes with large stakes from dominating the blockchain.

DOI: 10.54254/2754-1169/12/20230624

2.3. Comparing PoW & PoS

Even both methods have the same goal, which is choosing a new owner of the new block, it has differences between them. Proof-of-stake has advantages over proof-of-work, especially in terms of scalability and transaction speed. Proof-of-stake tokens are less harmful to the environment than proof-of-work. In contrast, Proof-of-Stake as relatively new technology has disadvantages in cybersecurity. The proof-of-work network requires a lot of resources such as mining hardware, electricity, etc., so the attack cost will be higher. This is especially true for Bitcoin, the largest proof-of-work blockchain.

Table 1: Comparing proof of work and proof of stake.

Pros for Proof of Work	**Pros for Proof of Stake**
Network Security	Scalability
Decentralized Method of verifying	Enhancing decentralization
	Energy Efficient
	Reduced transactions fee
	Faster confirmation time
	Anyone can Participate
Cons for Proof of Work	**Cons for Proof of Stake**
Relatively Slow	Relatively new
Extremely energy-intensive	Reward is not as much as mining

3. Case Study: Ethereum Converted to PoS

3.1. What is Ethereum

Ethereum is the second largest cryptocurrency after Bitcoin, which is also a blockchain-based platform. Bitcoin proves that a currency can be created by a community that anyone can send and receive through a cryptocurrency wallet, and it also solves the "double spend problem." What Ethereum proves is that blockchain is more than just a store of value. It can also put ideas, money, services, and more, into code and execute through smart contracts.

Ether (ETH) is the cryptocurrency Ethereum uses to build and maintain the operation of its network. It works similarly to Bitcoin, where miners create ETH by creating blocks and solving puzzles.

3.2. Ethereum's Proof of Works' Disadvantages

The Ethereum foundation proposed that they will be changed into a PoS consensus mechanism around April 2021, and this will most likely be taken place in September [5]. As discussed above, even PoW consensus mechanism has been dominant in the entire cryptocurrency market, there is no best consensus mechanism [6].

Proof of Work has been showing an advantage in many aspects, especially in high security. However, PoW has shown weaknesses in many different aspects that are influential in Ethereum's future - the well-known energy-intensive issue. Ethereum consumes around 75 TWh of energy per year; Bitcoin, on the other hand, consumes 152 TWh per year, and 75 TWh is 0.32% of the entire world's electricity consumption [7]. With this being said, the energy issue is the most significant related to the drawbacks of the Proof of Work consensus mechanism. This issue is not only caused by the company which used a proof-of-work algorithm that required thousands of mining hardware

DOI: 10.54254/2754-1169/12/20230624

devices to run continuously to support and secure the network, but also all the miners who are competing to get the new bitcoin using advanced mining-specialized equipment. There are more little problems related to Proof of Work consensus mechanism that is crucial to Ethereum, which will be addressed in the following.

3.3. Benefit of Converting to Proof of Stake

3.3.1. Environmental Issue

Around December 2020, the Beacon chain was launched by Ethereum [8]. This new Chain is essentially the new Ethereum. The Beacon Chain is a blockchain that uses the proof of stake consensus mechanism. Validators add blocks to the beacon chain, but these blocks do not contain any data or transactions. The merger requires transferring data stored on the Ethereum main net to the beacon chain, making the beacon chain the main blockchain on the Ethereum network.

The proof-of-stake algorithm reduces the resource consumption caused by mathematical operations to a certain extent, and the performance has also been improved accordingly. At the same time, proof of stake can also reduce the environmental burden. As cryptocurrencies gain wider adoption, it has created a considerable carbon footprint. Proof of Stake consensus mechanism significantly reduces this environmental cost by removing complex computation brought by PoW. Furthermore, with a successful transition from PoW to PoS, cryptographic puzzles will no longer be part of its network system. As a result, electricity spending on Ethereum is expected to drop by around 99.95%, according to the Ethereum Foundation [9]. The current global energy system is in turmoil, and the energy supply crunch has been in severe shortage, which has led to electricity and fuel prices having soared. This huge step Ethereum takes will help reduce energy consumption a lot since using 0.32% of the world's electricity is creating too much burden on the environment [7].

3.3.2. Low Transaction Cost and Faster Confirmation Speed

Ethereum, with the proof of work consensus mechanism, confirmation speed is around 15 seconds to 5 minutes.[10] Compared to other cryptocurrencies, it is a relatively long time, especially when Ethereum has to incorporate the smart contract, which requires a faster confirmation speed. In this case, they are processing much fewer transactions from the requirement of the smart contract system. Adding to that, each network confirmation requires a certain transaction fee, and it is called a gas fee in Ethereum. The amount of this fee is determined by auction. The higher the bid, the higher the request will be confirmed, while the request with the lower bid can only wait for even longer. Therefore, when the market was relatively hot last year, the gas fee confirmed by a contract was as high as tens or even hundreds of dollars. Therefore, after converting to PoS consensus mechanism, the efficiency of network confirmation will be increased, and the cost of using the Ethereum network will also be reduced.

4. Conclusion

With close analysis of the Proof of Work and Proof of Stake consensus mechanism, these two mechanisms have significant advantages and drawbacks over the other. Along with the implementation of this comparison onto the current Ethereum model, it can see that Ethereum's shift to PoS has indeed reduced the drawbacks of the Proof of Work consensus mechanism, mainly in terms of energy consumption, transaction cost, and confirmation speed. Therefore, Ethereum's shift to Proof of Stake is an intelligent move towards a greener future. In the future, after getting enough data from the after-merged Ethereum, it can be clearer to see if converting to Proof of Stake was a good move for Ethereum. Especially some in-depth research in the three aspects mentioned above.

DOI: 10.54254/2754-1169/12/20230624

Acknowledgement

I am thankful for all the papers published online for reference. Throughout the research, I have learned more than what I have written in this paper. There are so many good ideas being published on the internet, and I am grateful to all the authors that published those papers.

References

[1] *N. Lachtar, A. A. Elkhail, A. Bacha and H. Malik, "A Cross-Stack Approach Towards Defending Against Cryptojacking," in IEEE Computer Architecture Letters, vol. 19, no. 2, pp. 126-129, 1 July-Dec. 2020, doi: 10.1109/LCA.2020.3017457.*

[2] *Shi, N. A new proof-of-work mechanism for bitcoin. Financ Innov 2, 31 (2016). https://doi.org/10.1186/s40854-016-0045-6.*

[3] *Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017, August). Ouroboros: A provably secure proof-of-stake blockchain protocol. In Annual international cryptology conference (pp. 357-388). Springer, Cham.*

[4] *Tasca, Paolo; Tessone, Claudio J. (2019-02-15). "A Taxonomy of Blockchain Technologies: Principles of Identification and Classification". Ledger. 4. doi:10.5195/ledger.2019.140. ISSN 2379-5980.*

[5] *Lau, Yvonne (2021-05-27). "Ethereum founder Vitalik Buterin says long-awaited shift to 'proof-of-stake' could solve environmental woes". Forbes. Retrieved 2021-05-29.*

[6] *Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016, October). On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 3-16).*

[7] *Reeder, T. (2021, October 1). The truth about bitcoin and Ethereum energy consumption. Medium. Retrieved September 13, 2022, from https://medium.com/gochain/the-truth-about-bitcoin-and-ethereum-energy-consumption-20a325f39b52.*

[8] *Boom, D. V. (2022, September 12). Ethereum merge: Crypto's carbon footprint is about to shrink. CNET. Retrieved September 14, 2022, from https://www.cnet.com/personal-finance/crypto/countdown-to-ethereum-merge-what-it-is-and-why-its-important/.*

[9] *Ethereum. (2022, September 13). Ethereum Energy Consumption. ethereum.org. Retrieved September 14, 2022, from https://ethereum.org/en/energy-consumption/.*

[10] *Sergeenkov, A. (2022, April 13). How to check your ethereum transaction. CoinDesk Latest Headlines RSS. Retrieved September 14, 2022, from https://www.coindesk.com/learn/how-to-check-your-ethereum-transaction/.*