International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I4P220

Volume 69 Issue 4, 139-141, April 2021
© 2021 Seventh Sense Research Group®

# Survey on Blockchain Evolution and Proof-of-Stake Consensus Algorithm

Myung-Suk Lee[1], Kee-Joo Kim[2,*]

[1, 2] *Tabulra Rasa College, Keimyung University,*
*1035 Dalgubeol-daero, Sindang-dong, Dalseo-gu, Daegu, South Korea*

*zonoz@gw.kmu.ac.kr*

**Abstract** – *Blockchain has been steadily evolving and is used across various applications owing to its transparency, decentralization, immutability, and reliability characteristics. In this research, we have summarized the technological evolution of blockchain and investigated the principle of the proof-of-stake (PoS) algorithm among blockchain consensus algorithms and potential problems. As a research method, blockchain evolution is summarized based on the generation, and the principle of block creation and various attack vectors in the PoS algorithm are investigated. While the proof-of-work method has been applied to Bitcoin and its stability proven through numerous tests in practice, the PoS method has not yet been rigorously tested. As PoS has been drawing attention as a new consensus algorithm, we herein predict and review its potential drawbacks and problems.*

**Keywords:** *Blockchain, Proof-of-Stake, Consensus Algorithm, Blockchain Evolution.*

## I. INTRODUCTION

All forms of community, whether big or small, inevitably have an “Algorithm” that needs to be formed and retained. It works with relations between members of the community or with other communities beyond the said community. The relation encompasses not only the commercial relation required for the transaction but also social or political relations required for cooperation. This can be called a “Consensus Algorithm” in terms of a method and a system of establishing trust or consensus with members or people beyond them. This “Consensus Algorithm” refers to a method or a system that overcomes situations wherein opinions or interests differ or are in conflict, actively draws consensus, and passively resolves conflicts. This is because no community can be formed or retained without having a basis for generating consensus or trust. Simultaneously, sudden changes in the conditions of life or members of the community act as an element that fundamentally changes the “Consensus Algorithm.” In particular, the fundamental changes of the “Consensus Algorithm” that we are currently working on are implied in some of the new technologies, including blockchain, that brings about rapid changes in the way in which we live and behave. Among them, blockchain itself already qualifies as a new “Consensus Algorithm.” This is because it is the basis and method for creating consensus or trust. The unstable consensus of members in the community is now incorporated into the system. It is called blockchain, and although it is not yet a perfect algorithm, it gradually evolves with technological advances. Therefore, the evolution of blockchain technology and the proof-of-stake (PoS) algorithm, among the algorithms that draw consensus therein, will be examined in this research.

## II. BLOCKCHAIN EVOLUTION

Blockchain technology is evolving rapidly. The first-generation blockchain was applied to cryptocurrency Bitcoin, which began with Satoshi Nakamoto's paper in 2008[1], and it validates the current blockchain with an algorithm called the proof-of-work (PoW)[2] algorithm for consensus and a digital signature that encrypts the hash values with a private key for trust. The PoW algorithm, as a consensus algorithm, was difficult to apply to various industries owing to limitations such as transaction speed, processing capacity, and energy inefficiency. Second-generation blockchain began with Vitalik Buterin’s Ethereum[3] in 2015, and it proposed the concept of PoS in which the stake is used to reach a consensus. In addition, smart contracts were introduced to go beyond being a simple cryptocurrency and include assets such as loans and contracts in blocks. As the online smart-contract system is automated, the financial world, which has been providing credit services on the basis of money and contract for thousands of years, is in trouble. Finally, in September 2015, global financial institutions built an R3 consortium to accommodate virtual currency and smart contracts; as of May 2018, over 200 member companies have decided to build the R3 consortium and launched the Hyperledger Fabric 1.0[4] system on the market, which was considered the beginning of the third-generation blockchain. Although the blockchain was previously a public blockchain where anyone could participate in blockchain activities, Hyperledger is a permissioned blockchain that only allows authorized members to participate in blockchain activities. In other words, as was mentioned by Brian Behlendorf [5], a party that manages the blockchain network was created. Although the introduction of Hyperledger, which is the innovation of third-generation blockchain, has been transformed into a form different from the original spirit of the blockchain, it is expected to be a clue that addresses the limitations of the decentralization and trust structure of the blockchain as it must be developed from the part that can be applied to real-world socioeconomic systems.

**Table 1. Blockchain evolution**

| **Blockchain generation** | **1.0 generation** | **2.0 generation** | **3.0 generation** |
|---|---|---|---|
| **Developer** | 2008 Satoshi Nakamoto | 2015 Vitalik Buterin | 2018 (mentioned 3.0) Melanie Swan |
| **Consensus algorithm** | PoW | PoS, Ethash | DPoS, PBFT, IPoS, Kafka, Zookeeper |
| **Application** | Bitcoin(distributed ledger) | Ethereum(smart contract) | DApp |
| **TPS** | 4 TPS–10 TPS | 15 TPS–20 TPS | 100,000 TPS (Hyperledger), 3,000 TPS (EOS) |
| **Access permission** | Public Blockchain | Private Blockchain | Consortium Blockchain |
| **Platform development language** | Solidity | Solidity | Java, Python, etc. |
| **Limitation** | Limited application (virtual currency)<br>Transaction speed, processing capacity, interoperability<br>Malicious 51% attack vulnerability<br>Centralization based on computing power in PoW<br>Scalability and safety | The limited ripple effect on the commercialization market<br>Technical limitations and drawbacks<br>Transaction speed, an expensive fee paid by the user<br>Centralization based on the amount of stake in PoS<br>Scalability, safety, and decentralization | DPoS has low security and is vulnerable to attack against agents<br>PBFT decreases performance as nodes increase<br>As considerable authority is given to a small number of block creators, the collision between some of the 21 block creators can cause serious problems (EOS). |
| **Governance** | Hard fork caused ecosystem fragmentation | Issues due to lack of governance<br>DAO hacking led to hard fork divide into Ethereum Classic and Ethereum | Hyperledger Fabric is a private blockchain free from governance issues.<br>No hard fork in EOS |
| **Block creation time** | 10 min | 10-15 s | 0.5 s |
| **Blockchain examples** | Bitcoin, Litecoin, Monero, Ripple | Ethereum, Steemit, Ethereum Classic, NXT | Hyperledger, EOS, QTUM, NEO, IOTA |

## III. PROOF-OF-STAKE CONSENSUS ALGORITHM

### *A. Consensus Problem*

In the digital world, the double-spending issue occurs, which is a failure to distinguish between the original and the copy due to digital copying. For example, if A, whose total assets are 1 dollar, sends a transaction notice saying that A will transfer 1 dollar to B while simultaneously sending a transaction saying that it will transfer 1 dollar to C; moreover, if a consensus is not reached on which transaction is the valid one in the blockchain system, the same value will be paid twice. In the past, the data management authority was delegated to a trusted third party such as the bank to address this double-spending issue, but this also has a "third-party issue," such as commission fees, transaction delays, and single point of failure. On the contrary, the blockchain guarantees no errors and the integrity of the database without a third party or a central control system, even on a P2P network through the consensus algorithm. In other words, multiple peers (nodes) on the P2P network maintain a single database (blockchain) by reaching a consensus. This consensus algorithm is a command that controls how the node processes new transaction data and blocks.

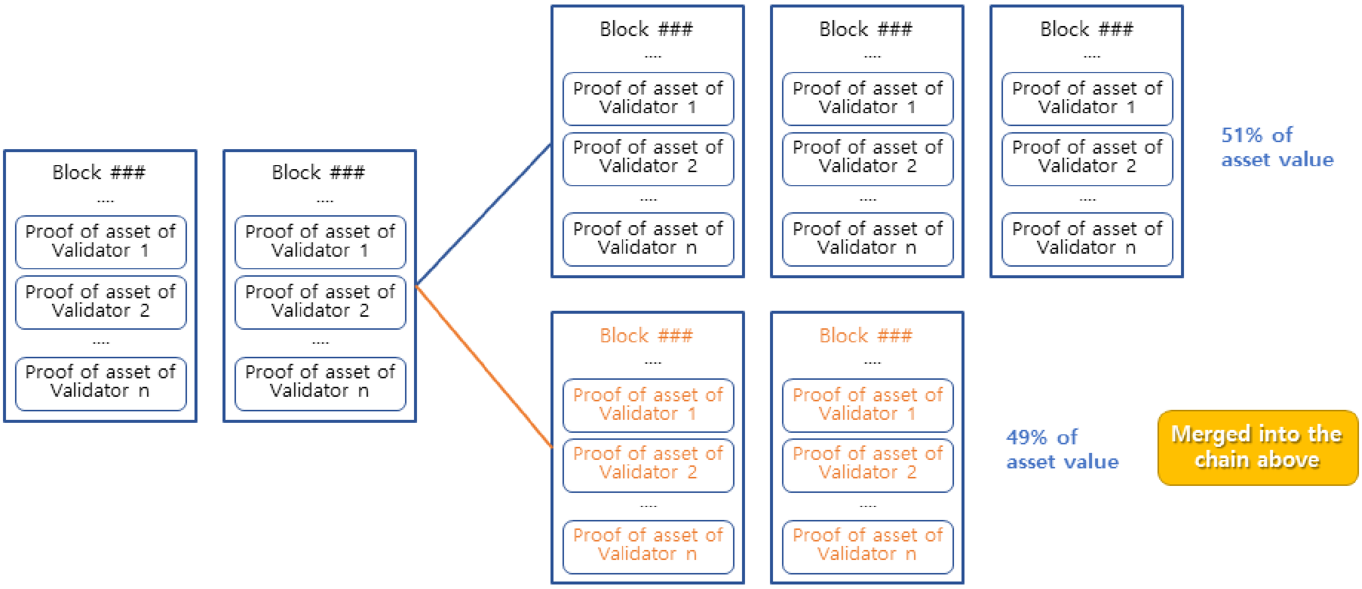
Block ###
....
Proof of asset of Validator 1
Proof of asset of Validator 2
....
Proof of asset of Validator n
51% of asset value
49% of asset value
Merged into the chain above

**Figure 1. PoS block creation**

### *B. Consensus Algorithm*

The consensus algorithm generally refers to an algorithm used by multiple participants to make unified decisions. In other words, the consensus algorithm is a way to reach a consensus among the untrusted parties. In a blockchain, the consensus algorithm maintains the integrity and security of the decentralized system, and this is a core element of the network. Basically, in a blockchain network, as all participants distribute and store data and these are decentralized, there is no need to make unified decisions. In such an environment, an algorithm that guarantees the integrity of the system is required as the trustworthy relationship between the nodes is lacking [6]. This is where the consensus algorithm begins. The consensus algorithm confirms whether the protocol rules are well followed and ensures that all transactions proceed in a reliable manner so that the coin is used only once [7].

### *C. Proof-of-Stake Block Creation*

In PoS, the authority to record on the block is given in proportion to the amount of stake instead of the work. All nodes that hold coins can add blockchain data through the consensus. In PoS, the rewards are earned in the concept of interest on the stake when a block is created. The point in time when the PoS block is created is shown in Figure 1.

The participant agrees to the block that they think is valid, and it displays and proves their stake on that block [8]. In the case of a fork, it is combined into the upper chain if the suggested value is 51% for the upper chain and 49% for the lower chain. In the end, even in the case of a fork where the chain splits, the chain with more assets will eventually survive.

## IV. CONCLUSION

If the key point was that in the PoW of the blockchain, a consensus is reached based on the computational power of the computer and more authority to record on the block is provided based on the speed of the computational power, the PoS is a theory that gives more authority to record on blocks in proportion to the number of stakes (corresponding coins) it holds, rather than the work. If more authority is given to record in the ledger to a person who simply holds more stakes, there is a risk of malicious attacks. Nevertheless, many developers prefer PoS to PoW as it is more energy-efficient compared to the PoW and can shorten the consensus process. This means that it is more difficult to centralize in PoS as it costs approximately 100 trillion to have 51% of the world's assets in PoS if it costs 1 trillion to have 51% hash power in PoW. Decentralization may be easier as more people can get involved in the decision-making process as any node with coins can access the network without permission. However, there are many challenges to be overcome, such as issues with regard to scalability, attack vectors, and wrong incentives. The PoW method is an algorithm that is the basis of Bitcoin, and its stability has been proven through numerous tests in practice. As the PoS method is now attracting attention as a new consensus algorithm, we predicted and reviewed the potential weaknesses and issues of the PoS method.

## REFERENCES

[1] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, www.bitcoin.org,

[2] Proof-of-work system. Online: https://en.wikipedia.org/wiki/Proof-of-work_system (2020).

[3] Ethereum's Casper. Online: https://cyber.stanford.edu/sites/g/files/sbiybj9936/f/ethereum_ proof_of_stake_casper_ffg_2017_chronicles. pdf (2020)

[4] An Introduction to Hyperledger. Online: https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_Introductionto Hyperledger.pdf (2020).

[5] HashNet, http://wiki.hash.kr/index.php/brain_behlendorf (2020).

[6] Proof-of-stake. Online: https://en.wikipedia.org/wiki/Proof-of-stake (2020).

[7] M. S. Lee, K. J. Kim, A Survey on Consensus Algorithm of Blockchain: Focusing on PoW", Proceedings of KSCI Conference 28(2020) 567-570.

[8] Banksalad, https://banksalad.com/contents/lr7RH (2020).