



Proof of Stake Beyond Wealth: A Novel Blockchain Consensus Algorithm

Vinola C¹, Naveen Rajan M², Guruprasath M³, Mounasri V⁴

¹Associate Professor and Head, Department of CSE (IoT, CS including BCT), Sri Sairam College of Engineering, Anekal, Bengaluru-562106

^{2, 3, 4}Third Year students, Department of CSE, Sri Sairam College of Engineering, Anekal, Bengaluru-562106

ABSTRACT

This research paper addresses the limitations of the Proof of Stake (PoS) consensus mechanism in blockchain technology. Consensus is the foundational element of blockchain, and two of the most widely discussed mechanisms are Proof of Work (PoW) and PoS. While PoS offers advantages over PoW, it also presents significant challenges, notably wealth concentration. This paper investigates these limitations in depth and proposes a novel framework aimed at mitigating these issues. By exploring the dynamics of stake distribution and validator incentives, this study seeks to enhance the security and fairness of PoS systems.

Keywords: Consensus, Blockchain, Proof of Stake

1 Introduction

Blockchain technology has emerged as a transformative force in the realm of Web 3.0. Initially conceptualized by the pseudonymous Satoshi Nakamoto in 2009 to support the Bitcoin network, blockchain has since evolved into a foundational element for a wide range of applications beyond cryptocurrencies. The launch of the Ethereum (ETH) network in 2015 marked a significant milestone in this evolution, addressing the limitations of Bitcoin by introducing smart contracts and enabling decentralized applications (dApps). Additionally, Ethereum overcame the constraints of the Proof of Work (PoW) consensus mechanism by implementing Proof of Stake (PoS), further enhancing scalability and energy efficiency. Let's delve further in addressing the limits of this PoS.

2 Recent Works

Limits of PoS [proof of stake] [5]

While Proof of Stake (PoS) offers several advantages over Proof of Work (PoW), it also presents its own set of challenges. One major concern is the tendency for wealth concentration, where individuals or entities with greater financial resources are able to accumulate more stakes, thus gaining disproportionate influence over the network.

Wealth concentrated [4]

In the Proof of Stake (PoS) consensus mechanism, validator nodes engage in a process to validate new transactions and add them to the blockchain. Each validator stakes a certain amount of cryptocurrency, and a voting algorithm determines which validator is selected to



propose a new block. In this system, validators who stake larger amounts have a higher probability of being chosen to validate new transactions and propose blocks. Consequently, individuals or entities with significant financial resources are afforded more opportunities to participate in this process than those with smaller stakes.

This concentration of wealth can lead to security implications, as it may undermine the decentralized nature of the network. When a small number of wealthy validators hold disproportionate power, it raises concerns about potential collusion, manipulation of the network, and reduced overall security.

Current Validator election [2]

In a Proof of Stake (PoS) blockchain network, validators play a crucial role in maintaining the integrity and security of the blockchain. The process of validator election, block proposal, and consensus is structured around epochs and slots, ensuring an efficient and democratic approach to block creation and validation.

Structure of Epochs and Slots

Validators are grouped into “epochs”, which consist of a defined number of “slots”. Each slot represents a specific time frame during which a block can be proposed. This organization allows for systematic block production and validator participation.

2.1 Selection of Block Proposers

At the beginning of each slot, a block proposer is chosen through an election mechanism. This selection is heavily influenced by the amount of cryptocurrency that validators have staked in the network. Validators with larger stakes have a higher likelihood of being elected as block proposers, giving them more opportunities to create and propose new blocks.

Block Proposal and Transaction Selection

Once a validator is designated as the block proposer for a given slot, they will compile transactions from the mempool a collection of pending transactions waiting to be confirmed. The block proposer creates a new block containing these transactions and submits it for validation by other validators.

Attestation and Voting Process [2]

After the block has been proposed, other validators, known as attesters, participate in the voting process. They have the option to “approve” the proposed block or “deny” it. This voting mechanism ensures that all validators have a say in which blocks are added to the blockchain.

Consensus and Block Finalization [3]

The block that receives the highest number of approval votes from attesters is granted the right to be added to the blockchain. In many PoS networks, a supermajority of votes (often around two-thirds of the total stake) is required to finalize a block, ensuring robust consensus and minimizing the risk of forks.



Consensus under Pressure: The Tie Dilemma [7]

In a blockchain network, consensus can become particularly challenging when two blocks, proposed by different slots, receive an identical number of votes from attesters. This scenario places the network in a state of tension, as it must determine which block should be added to the blockchain.

When faced with such a tie, several strategies can be employed to reach a consensus

Forking: One possible outcome in the event of a tie is forking, where the blockchain splits into two separate chains, each containing one of the tied blocks. This can lead to temporary divergence in the network, with different validators potentially choosing to build on different versions of the blockchain. While forking allows for both blocks to exist simultaneously, it can introduce complications such as increased uncertainty and reduced trust among participants. Over time, the network may converge back to a single chain as validators favor one block over the other due to additional votes or confirmations.

Tie-Breaking Mechanisms: To mitigate the issues associated with forking, many blockchain protocols implement specific tie-breaking mechanisms designed to provide clarity in these situations. Common approaches include:

Random Selection: A random mechanism could determine which block to adopt, introducing an element of chance that promotes fairness among competing validators.

Stake Weight: Validators with larger stakes may have greater influence in the decision-making process. This can involve evaluating the total stake of validators backing each block, with the block that has the support of more significant staked assets being favored.

Chronological Order: In some networks, the block that was proposed first might be prioritized for inclusion in the blockchain, providing a straightforward resolution to the tie.

Secondary Voting: Another method could involve conducting a secondary round of voting among the attesters, specifically focused on resolving the tie.

The tie dilemma conclusion:

The current way of handling tie situations in blockchain voting can be slow and mostly depends on how much money validators have. This focus on wealth can create an imbalance, where those with more money have more control over decisions. As a result, the methods used to resolve conflicts may not truly reflect the views of everyone in the network.

This research aims to find new ways to solve voting conflicts that do not rely on wealth. By moving away from this focus, we hope to create fairer and more efficient ways to handle ties. Our goal is to develop a consensus process that includes all validators, regardless of their financial stake, making the blockchain system more resilient and fairer for everyone.

3 Proposed Work Explanation

The current way of resolving ties in blockchain voting focuses mainly on wealth, which can lead to unequal power among validators. To fix this problem, this paper suggests introducing a Credit-Based Proof of Stake (CpoS) system.

CpoS would give validators voting power based on their contributions to the network instead



of just their financial investments. Validators could earn credit by participating in decision-making, engaging with the community, and other positive actions. This would help ensure that everyone, no matter how much money they have, can have a say in important decisions.

By using a credit-based system, we can better handle tie situations and create a fairer blockchain ecosystem. This solution encourages more active participation from different validators and improves the fairness and strength of the consensus process.

3.1 How CPoS works

After every successful decision made by a validator, they will earn a certain amount of credits from the CPoS algorithm. These credits will assist in decision-making during the attestation process.

Handling Tie dilemma

When two blocks receive the same amount of votes, the tie dilemma occurs. In Credit-based Proof of Stake (CPoS), when a tie happens, it checks the voter's credits. Voter credits refer to the credits of each voter; for example, if a block receives 10 votes from attesters, it takes a list of the credits from all 10 voters.

An approximate analysis of expected ties per hour in Blockchain for every 12s there will be a new transaction in mempool waiting for validation.

Analysis:

Let transaction Time (t) = 12s number of transaction per hour, transaction (tx) = 3600s/t,

Total number of transaction per hour (tx) = 300 Tie dilemma:

According to the research the probability of occurrence of tie is 7.96%,

So,

Tie (p) = 0.0796

Expected ties for an hour (px) = p * tx

=> px ≈ 23.88 [24px]

Approximately there occurs 24 tie transaction per hour.

24 ties in 300 transactions, its relatively very low even then when it occurs it should be handles efficiently using this credit based pos(CpoS).

How CpoS handles Tie?:

Block A:	Block B:
10 attesters	10 attesters
[0A] 10credits	[0A] 7credits
[1A] 5credits	[1A] 3credits
[2A] 12credits	[2A] 10credits
.	.
.	.
[9A] 4credits	[9A] 8credits

For instance, let us consider a tie happened now CPoS takes the list of voters.

Now CpoS sums up the credits of voters in each block A: 10+5+12+...+4 credits



Block B: $7+3+10+\dots+8$ credits

Let us assume block A has 31 credits Block B has 28 credits.

So now the attester conflict is solved with credits not by wealth. Block A will proceed further because block A has more number of trusted attesters.

3.2 Effect of CPoS on Blockchain

- Security
- Network integrity
- Improved Trustworthy Behavior
- Incentivized Participation
- Decentralization

Since the Credit-based Proof of Stake (CPoS) model is centered around credits, validators receive credits only when they demonstrate honest behaviour. By earning these credits through our algorithm, we build a system that inherently trusts the validators who participate in the block validation process. This credit system not only incentivizes integrity but also fosters a more reliable network, as trusted validators contribute to maintaining the security and integrity of the blockchain.

Handling Dishonesty

In traditional Proof of Stake (PoS), a validator stakes a certain amount of cryptocurrency as collateral, which can be penalized if they act dishonestly.

3.3 CPoS

In Credit-based Proof of Stake (CPoS), validators are required to submit two forms of collateral: [1] cryptocurrency and [2] credits. While credits serve as a direct form of collateral that does not need to be explicitly submitted, validators must stake cryptocurrency to participate in the network. If a validator engages in malicious behavior, both their credits and staked cryptocurrency will be subject to slashing. This dual collateral system ensures that validators are incentivized to act honestly and maintain the integrity of the blockchain.

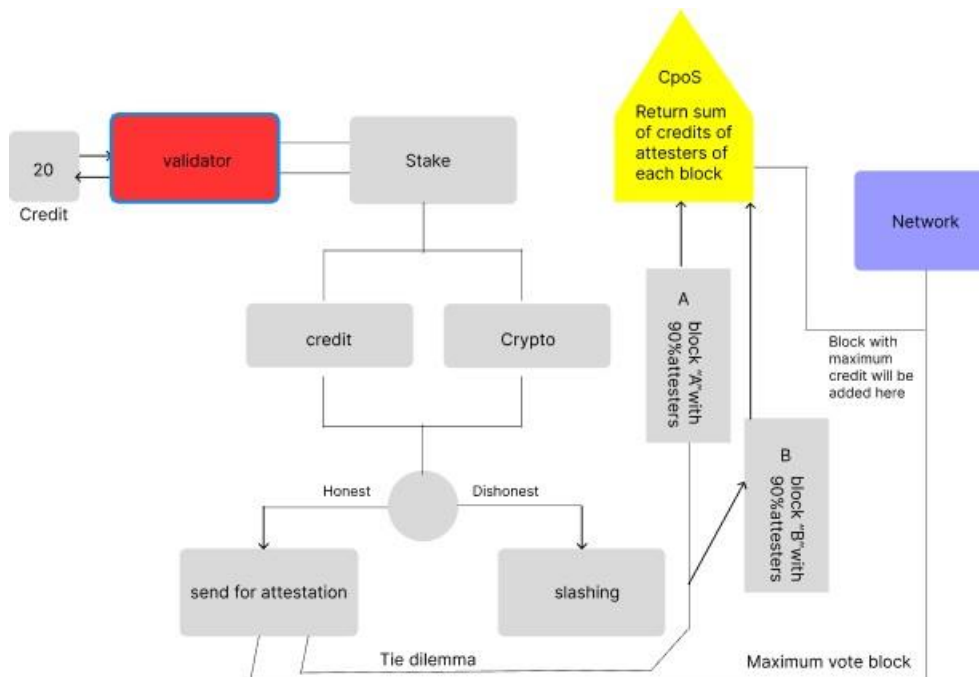


Figure 1: Proposed block diagram

4 Results and Conclusion

Credit-based Proof of Stake (CPoS) provides a new and improved way for reaching consensus by fixing some of the key problems in traditional PoS systems. CPoS uses both cryptocurrency and earned credits as forms of collateral, adding extra accountability. Validators earn credits for honest behavior, which increases their reputation and discourages dishonesty. Unlike regular PoS, which tends to favor those with more money, CPoS combines financial stake with earned credits, making the process fairer and less controlled by wealth. This combined approach not only improves security but also boosts trust in the blockchain, as validators are encouraged to act openly and responsibly. In the end, CPoS creates a more balanced, reliable, and efficient network, promoting long-term fairness and trust across the blockchain ecosystem.

References

1. Xuesen Zhang; Qinglei Guo; Xiaoxiao Ma; Zhe Du; Shuang Sun; Desheng Bai, Year: 2022, "Research on blockchain consensus algorithm for large-scale high-concurrency power transactions," 2022 9th International Forum on Electrical Engineering and Automation (IFEEA).
2. Aryan Trivedi; Hrithik Mistry; Yukti Shah; Ramchandra Mangrulkar; Nitin S. Goje; Parikshit Mahalle, Year: 2023, "Enhanced Schema for Proof of Stake Mechanism Based on Stake Size and Random Validator Selection," 2023 International Conference on Advanced Computing Technologies and Applications (ICACTA).



3. Amool Sudhan; Manisha J Nene, Year: 2018, "Peer Selection Techniques for Enhanced Transaction Propagation in Bitcoin Peer-to-Peer Network," 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS).
4. Yli-Huumo J; Ko D; Choi S; Park S; Smolander K, Year: 2016, "Where Is Current Research on Blockchain Technology?—A Systematic Review”.
5. Zibin Zheng; Shaoan Xie; Hongning Dai; Xiangping Chen; Huaimin Wang, Year: 2017, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (Big Data Congress).
6. Ethereum. <https://ethereum.org/>
7. Azbeg K; Ouchetto O; Jai Andaloussi S; Fetjah L, Year: 2021, “An overview of blockchain consensus algorithms: Comparison, challenges, and future directions”.
8. T. Al-Hadhrani; F. Mohammed; E. Mohammed, “Advances on smart and soft computing”, Advances in Intelligent Systems and Computing, Vol. 1188.
9. Sheng H; Fan X; Hu W; Liu X; Zhang K, Year: 2018, “Economic incentive structure for blockchain network”, In M. Qiu (Ed.), Smart Blockchain. Smart Block 2018. Lecture Notes in Computer Science, Vol. 11373.