AN EFFICIENT AND ROBUST PROOF OF STAKE ALGORITHM BASED ON COIN-AGE SELECTION

ANJANEYULU ENDURTHI[1], AKHIL KHARE[2]

[1]Research Scholar, Osmania University, Hyderabad, India & Assistant Manager (IT), Food Safety and Standards Authority of India, New Delhi, India

[2]Professor, CSED, Maturi Venkata Subba Rao Engineering College, Hyderabad, Telangana, India.

E-mail: [1]anjaneyuluendurthi@gmail.com, [2]khare_cse@mvsrec.edu.in

ABSTRACT

A consensus protocol is used to achieve agreement among the nodes in a distributed system. Proof of stake is one such protocol. Proof of stake is based upon two different strategies. The first one is randomized block selection and the second is coin-age selection. Each of these strategies results in an unfair selection of validators and converges to a problem called wealth concentration among a few validators. This paper proposes a modified proof of stake protocol based on the coin-age strategy to mitigate the issue and improve the coin-age selection algorithm. The participants will generate new tokens to compete for the validator role to create the next block.

Keywords: *Blockchain, Consensus, Proof of stake, Coin-age, Timestamp, Tokens*

1. INTRODUCTION

A blockchain [1] is a data structure that stores transactions in an immutable manner. The immutability of blockchain is achieved by using the cryptographic principles. The blocks in the blockchain are linked using a cryptographic hash. New blocks are added to the existing blockchain when a certain consensus is achieved among the nodes that are participating in the consensus process. Blockchain is decentralized [2] meaning that the complete blockchain is available with all the peers of the network and there is no central authority that controls the network and blockchain. Blockchain has a wide range of applications across all sectors. The applications are not limited to cryptocurrency, supply chain management, voting, smart contracts [3], healthcare [4] the entertainment industry, etc.

Each block of the blockchain consists of a hash to the previous block, Merkle root, hash of the block, timestamp, nonce, transactions or information, etc. Transactions are records of exchanges of value or information. Transactions can represent anything from cryptocurrency transfers to contract executions.

Following are some important steps that demonstrate the working and security of blockchain:

- ✓ Transactions: Participants exchange assets or information.
- ✓ Verification: Transactions are validated by network nodes.
- ✓ Block Formation: Valid transactions are grouped into blocks.
- ✓ Consensus: Agreement is reached on adding blocks to the chain.
- ✓ Block Addition: Validated blocks are added to the blockchain.
- ✓ Incentives: Participants are rewarded for contributing to the network.
- ✓ Decentralization: No single entity controls the network.
- ✓ Immutability: Transactions are irreversible and tamper-proof.
- ✓ Transparency: Transaction history is publicly accessible.

This process ensures a secure, transparent, and decentralized ledger system.

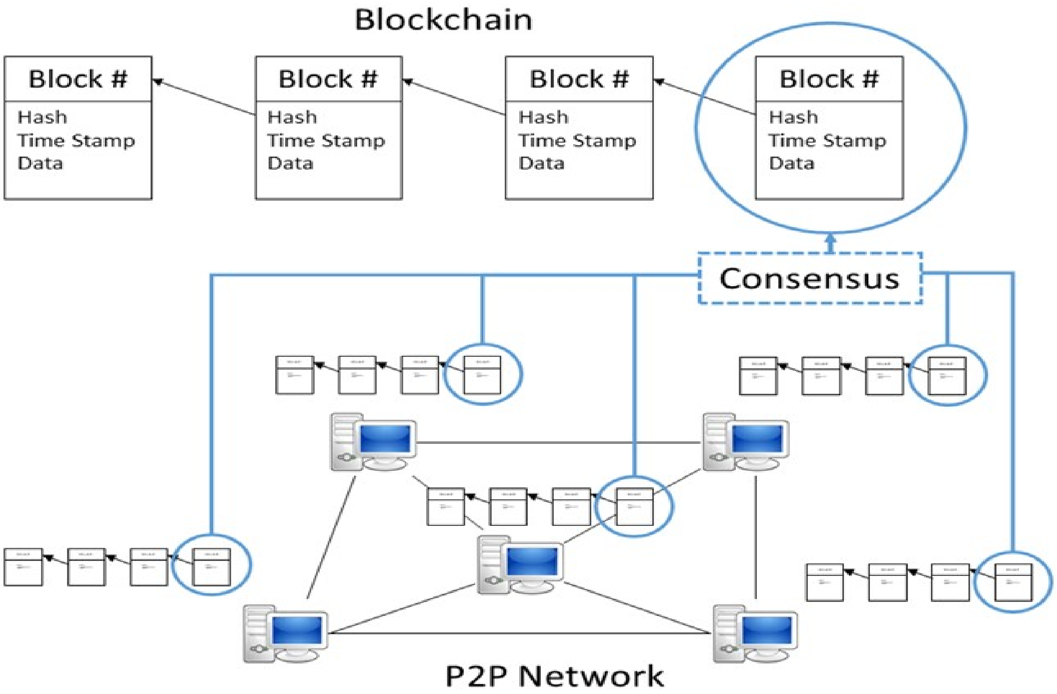


Figure 1: Blockchain, p2p network, and Consensus structure

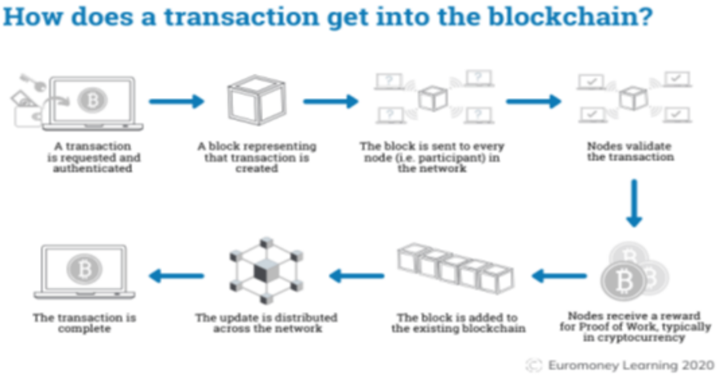

How does a transaction get into the blockchain?
A transaction is requested and authenticated
A block representing that transaction is created
The block is sent to every node (i.e. participant) in the network
Nodes validate the transaction
Nodes receive a reward for Proof of Work, typically in cryptocurrency
The block is added to the existing blockchain
The update is distributed across the network
The transaction is complete
© Euromoney Learning 2020

Figure 2: Working of Blockchain

The paper introduces a consensus algorithm based on the coin age selection criteria. Few parameters have been introduced and mathematically proved that the designed consensus algorithm more efficient and robust. In the proposed method, the nodes that are interested in becoming validators should mint staking tokens derived from the native tokens. The timestamp of these staked tokens is used as a critical parameter to calculate the hash power of the peers. The key assumptions in this study is the tokens being minted by each node before participating in the consensus process.

The outline of the paper is as follows: In the next section, literature review has been presented, section 3 discusses about the proposed methodology, the implementation, results are presented in section 4, In section 5, conclusion for the research is provided, future scope is presented in section 6 and finally the references.

2. LITERATURE REVIEW

There are many consensus algorithms [5] [6] [7] available in the literature. Each of them has their pros and cons. Some of the majorly used consensus algorithms are – Proof of work [1], Proof of stake [8] [9], Delegated proof of stake [10], Proof of burn [11], Proof of Activity [12], Proof of Weight [13], Proof of elapsed time [14], Proof of Adjourn [15], Delegated byzantine fault tolerance problem [16] etc.

2.1 Proof of Work

The proof of work consensus algorithm was coined by Satoshi Nakamoto [1], the creator of Bitcoin cryptocurrency. With the help of proof of work consensus protocol, Satoshi has successfully established trust in a decentralized system.

In proof of work, the transactions are bundled into blocks by the network participants known as Miners. These miners compete to generate a nonce such that the hash of the current block is less than the hash (target hash) produced by the network. The hashes are calculated by using the double SHA-256 function in the case of Bitcoin. The nonce generated by the miner is verified by the other network participants. If the nonce and generated hash satisfy the requirements, the created block is then added to the existing blockchain and the miner gets rewarded with bitcoins. The reward currently is 6.25 BTC for each block created and this will be halved to 3.125 BTC around April 20, 2024. Along with this reward, the miners will also get a transaction fee from the peers who have placed the transactions.

As miners are competing to find the hash, the computing power of all other miners who didn’t become successful in mining the block, gets wasted as only one miner gets successful and gets rewarded. Along with the wastage of computing power of the miners, there are many other drawbacks associated with proof of work consensus protocol. in the field may be eligible.

2.2 Proof of Stake

Proof of Stake (PoS) [17] [18] [19] is another consensus protocol for achieving consensus among peers in a decentralized system. Unlike proof of work, where miners compete with each other to find a hash and thus nonce, proof of stake selects a validator based on the stake promised by the network participants and this validator is responsible for adding a new block in the existing blockchain. As per proof of stake, the peers holding x% of the cryptocurrency can validate x% of the blocks, if they are interested in the validation procedure.

Depending on the number of tokens (amount of cryptocurrency) the participants are staking, the network selects one participant as the validator and this validator is responsible for creating the next block and adding it to the blockchain. I the validator fails to create a valid block, the staked amount will not be transferred back to the validator and it is considered a penalty for creating the invalid block otherwise after the successful creation of a valid block, the staked amount along with the reward (for creating the new block) will be transferred to the validator.

PoS typically achieves faster transaction confirmations and finality compared to PoW, as there is no need to wait for multiple confirmations from subsequent blocks. validators risk losing their staked cryptocurrency if they act maliciously or validate invalid transactions. This economic incentive encourages honest behaviour and secures the network against attacks. PoS is often praised for its energy efficiency compared to PoW as only one validator who was chosen will be creating the block.

While PoS has several advantages over PoW, including lower energy consumption and potentially higher scalability, it also has its own set of challenges [20] and criticisms. These include the "nothing at stake" problem, where validators have little to lose by validating multiple conflicting chains, and the potential for centralization among wealthy stakeholders.

Proof of Work and Proof of Stake [21] [22] [23] has continued to evolve with ongoing research and developments [24] within the blockchain space. some recent trends and advancements in PoS are as follows –

2.2.1 Ethereum 2.0

One of the most significant developments in PoS is Ethereum's [25] [26] [27] transition from Proof of Work (PoW) to PoS with the Ethereum 2.0 upgrade. This upgrade has resulted in solving the scalability issues and substantially reduced the energy consumption by Ethereum mining. Ethereum 2.0 introduces the Beacon Chain, which acts as the PoS consensus layer, while the existing Ethereum network (Eth1) continues to operate as a PoW chain during the transition period. Ethereum's move to PoS has been highly anticipated and could have significant implications for the broader blockchain ecosystem.

2.2.2 Cosmos (Tendermint)

Cosmos [28] is another prominent blockchain project that utilizes a PoS consensus mechanism called Tendermint. Tendermint is designed to achieve fast block times and high throughput while maintaining security through Byzantine Fault Tolerance (BFT). Cosmos aims to create an interoperable ecosystem of independent blockchains, known as zones, secured by the Tendermint consensus engine.

2.2.3 Polkadot

Polkadot [29] is a multi-chain interoperability protocol that also employs PoS as its underlying consensus mechanism. Polkadot's relay chain uses PoS to validate transactions and secure the network. Polkadot's design allows for the interoperability of diverse blockchains, known as parachains, which can connect to the relay chain for shared security and communication.

2.2.4 Tezos

Tezos [30] [31] is a self-amending blockchain application. The underlying consensus mechanism in Tezos is called Liquid Proof of Stake (LPoS) which is one of the variants of PoS. The validators here are called as Bakers.

2.2.5 Research and Innovations

One of the most significant developments in PoS is Ethereum's [25] [26] [27] transition from Proof of Work (PoW) to PoS with the Ethereum 2.0 Research and Innovations: Beyond specific projects, ongoing research and innovations in PoS focus on addressing its limitations and improving its scalability, security, and decentralization. This includes advancements in consensus algorithms, economic incentives, governance mechanisms, and sustainability initiatives.

Overall, PoS continues to be a prominent area of interest and development within the blockchain community, with various projects exploring its potential to create more efficient, scalable, and secure decentralized networks.

Even though PoS has many pros than PoW, it still has many setbacks and challenges that need to be addressed. Following are some of the challenges concerning proof of stake.

2.2.6 Wealth Concentration

PoS systems allocate block creation and validation privileges based on the cryptocurrency held and staked by participants. It can lead to wealth concentration, where a small group of stakeholders with significant holdings has disproportionate influence over the network. Such concentration could potentially lead to centralization concerns, where powerful stakeholders may dominate decision-making processes and control the network.

2.2.7 Nothing at Stake Problem

The "nothing at stake" problem [32] comes in PoS when validators have little to lose by supporting multiple competing blockchain forks simultaneously. Unlike PoW, where miners must invest resources in one chain at a time, PoS validators can theoretically support multiple forks without risking anything. This behaviour could undermine the security and finality of the blockchain, as validators may not have strong incentives to converge on a single valid chain.

2.2.8 Long-Term Security Risks

PoS systems rely on economic incentives to ensure the validity of the network. If the value of the staked cryptocurrency significantly decreases or if the cost of attacking the network becomes economically feasible, the security of the PoS blockchain could be compromised. Additionally, PoS networks may be vulnerable to attacks such as "nothing at stake", “long-range”, and censorship attacks, which could undermine trust in the system.

2.2.9 Centralization Pressures

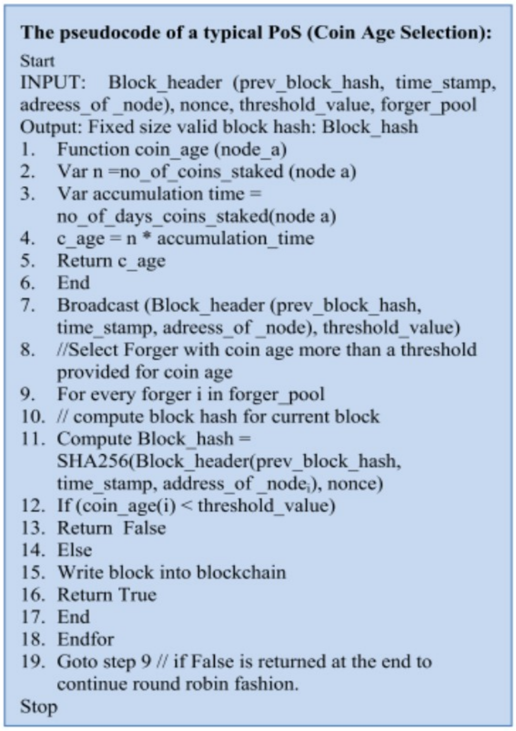
PoS is often touted as more energy-efficient than PoW, it still faces centralization pressures, albeit of a different nature. In PoS, validators with larger stakes typically have a higher probability of being selected to create and validate blocks. This can lead to centralization as larger stakeholders may have more resources to invest in infrastructure, thereby increasing their chances of being selected as validators. Centralization can undermine the decentralization and censorship-resistant properties of blockchain networks.

2.2.10 Initial Distribution Challenges

PoS networks require an initial distribution of tokens to bootstrap the system and ensure decentralization. However, achieving a fair and equitable distribution of tokens can be challenging, as early adopters or stakeholders may disproportionately benefit from the system's growth. Uneven token distribution could exacerbate wealth concentration and centralization concerns, particularly if a small group of stakeholders controls a significant portion of the token supply.

Despite these drawbacks, PoS continues to be a topic of active research within the blockchain community.

The pseudocode [33] for the proof of stake using coin-age selection is given below:



The pseudocode of a typical PoS (Coin Age Selection):

```
Start
INPUT:   Block_header (prev_block_hash, time_stamp,
adreess_of _node), nonce, threshold_value, forger_pool
Output: Fixed size valid block hash: Block_hash
1.  Function coin_age (node_a)
2.  Var n =no_of_coins_staked (node a)
3.  Var accumulation time =
    no_of_days_coins_staked(node a)
4.  c_age = n * accumulation_time
5.  Return c_age
6.  End
7.  Broadcast (Block_header (prev_block_hash,
    time_stamp, adreess_of _node), threshold_value)
8.  //Select Forger with coin age more than a threshold
    provided for coin age
9.  For every forger i in forger_pool
10. // compute block hash for current block
11. Compute Block_hash =
    SHA256(Block_header(prev_block_hash,
    time_stamp, address_of _node_i), nonce)
12. If (coin_age(i) < threshold_value)
13. Return  False
14. Else
15. Write block into blockchain
16. Return True
17. End
18. Endfor
19. Goto step 9 // if False is returned at the end to
    continue round robin fashion.
Stop
```

Figure 3: pseudocode for the proof of stake using coin-age selection

3. PROPOSED METHODOLOGY

In contrast to previous algorithms built upon the Proof of Stake (PoS) Protocol, such as coin age and randomized block selection, this method incorporates timestamps to compute a unique value (hash power) for each validator. These values are then utilized as probability scores to randomly select a validator. Consequently, validators with higher scores stand a greater chance of selection, and the uniqueness of these scores, compared to other methods, ensures fair selection.

In traditional approaches, native tokens are staked directly for participation in validator elections. However, in the proposed method, the nodes that are interested in becoming validators should mint staking tokens derived from the native tokens. The timestamp of these staked tokens is used as a critical parameter to calculate the hash power of the peers.

The procedure for the same is given below:

- ✓ A node seeking validator status initiates the creation of new tokens.
- ✓ The newly created tokens are staked by the participants if they are interested in becoming the validator.
- ✓ Each validator's hash power is computed using the method outlined in the subsequent section.
- ✓ The hash power is used as a parameter to build the pie chart, facilitating visualization of the probabilities.
- ✓ This pie chart is akin to a roulette wheel which is spun around randomly to select a validator. Thus, those with greater hash power possess higher probabilities of being elected as the validator to create the next block.
- ✓ After creating the new block, the tokens that were staked earlier are redistributed to all participating peers. Timestamps are applied based on whether the node emerged victorious or not.

The hash power of each node can be calculated using the following formula:

$$Hp = N * (Te - Ts)$$

Figure 4: Hash power calculation

In this context:

Hp represents the hash power,
N denotes the number of tokens staked by the node,
Te signifies the time of election (epoch), and
Ts represents the staked tokens timestamp (epoch).

Given that staked tokens may not always share the same timestamp, the formula can be modified as follows to accommodate tokens with multiple timestamps:

$$Hp = \sum_{i=1}^{n} = Ni\left|(Te - Tsi)\right|$$

Figure 5: Hash power calculation for multiple timestamps

In this context:
Hp and Te retain their definitions as previously described.
i represents the number of staked tokens.
Ni and Tsi denote the election time and tokens timestamp, respectively, for the ith record.

To mitigate the potential dominance of token timestamps and their disproportionate contribution to hash power, a limit is imposed on the validity of staking tokens. These tokens remain valid for a duration of 'i' days from their minted date. Should the minted tokens go unused within this timeframe, they are returned to the node that initiated their minting. For simulation purposes, the value of 'i' is set to 10 days. While there is no specific rationale for choosing this value, it is selected to enhance the efficiency of the proposed method. Considering that coin-age previously imposed a limit of 30 days, a value of '10' days is deemed sufficient for the intended purpose.

The new timestamps can be calculated as per the following procedure:

If the stake is returned to the nodes with the previous timestamps, it will lead to the same hash power calculation thus resulting in the "rich getting richer" phenomenon as the same node may win in the future validator elections. In the proposed approach, the tokens are returned to the nodes with a distinct timestamp. There are two cases for giving distinct timestamps. The first case applies to the node who has won the previous election and has become a validator and the second case applies to all the other nodes who lost the previous elections. This is to achieve fairness in the protocol.

- ✓ Case 1: Timestamp calculation for the previous winner can be calculated as per the below formula

$$Wt = Te$$

Figure 6: Timestamp calculation – winner tokens

In this context:
Wt = Timestamp of the winner
Te = Date and time of election (epoch)

- ✓ Case 2: Timestamp calculation for the previous losers can be calculated as per the below formula

$$Lt = (Te + Ts)/2$$

Figure 7: Timestamp calculation – winner tokens

The above formula gives the mean of the previous timestamp and election time.
In this context:
Lt = Timestamp of the losers
Te = Date and time of election (epoch)
Ts = previous timestamp of tokens (epoch)

4. IMPLEMENTATION AND RESULTS

This section explains the results of the research and at the same time gives a comprehensive discussion. Results can be presented in figures, graphs, tables and others that make the reader understand easily. The discussion can be made in several sub-sections.

The main aim of implementing the idea is to understand by what probability the new method can increase the precision and randomness in selection of the validators to mine the next block.

It is tough to simulate the whole ideology on an active blockchain. Hence, we came up with the idea of having a smart contract that contains all the helper functions needed to implement the proposed methodology deployed in a local blockchain i.e. Ganache, that itself acts as a blockchain. It has all the records, blocks, transactions, etc. They all can be visualised through any front-end web application.

The below set of tools and technologies are used to simulate the whole concept that is proposed.

- ✓ Ganache
- ✓ Solidity
- ✓ Remix
- ✓ Vercel
- ✓ Postman

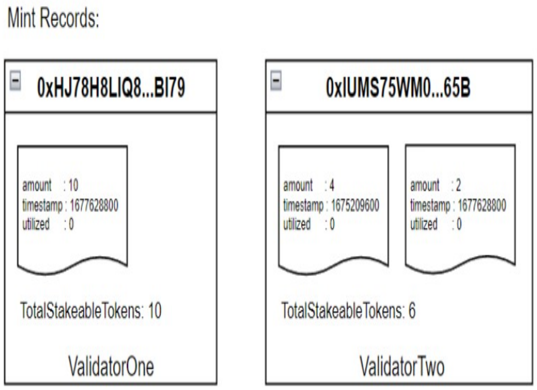
The Core Functionalities of the implementation are given below.

- ✓ Mint function
- ✓ Stake function
- ✓ Choose the Validator function
- ✓ Mine function

All these functions are implemented using the solidity programming language.

4.1. Mint function

This takes in timestamps and amounts as parameters. It is payable so equivalent to the amount, ethers should also be sent. On successful execution of this function, it stores the history. The minting of records for two validators is shown in figure 8.



Mint Records:

0xHJ78H8LIQ8...BI79

amount : 10
timestamp : 1677628800
utilized : 0

TotalStakeableTokens: 10

ValidatorOne

0xIUMS75WM0...65B

amount : 4
timestamp : 1675209600
utilized : 0

amount : 2
timestamp : 1677628800
utilized : 0

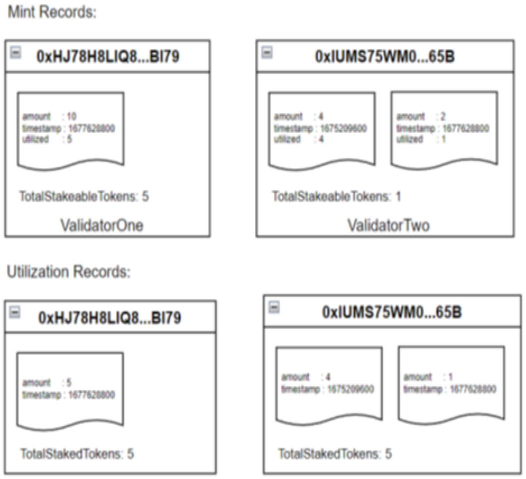
TotalStakeableTokens: 6

ValidatorTwo

Figure 8: Token minting for two validators

4.2. Stake function

This checks the total stackable tokens of a node and then stakes the amount passed as a parameter against that election. This runs an algorithm that groups the stackable tokens by timestamp and consumes the tokens from each record until the required amount is reached. Then for each consumption from the record, a utilisation record is generated. The staked tokens of two validators are presented in figure 9.



Mint Records:

0xHJ78H8LIQ8...BI79

amount : 10
timestamp : 1677628800
utilized : 5

TotalStakeableTokens: 5

ValidatorOne

0xIUMS75WM0...65B

amount : 4
timestamp : 1675209600
utilized : 4

amount : 2
timestamp : 1677628800
utilized : 1

TotalStakeableTokens: 1

ValidatorTwo

Utilization Records:

0xHJ78H8LIQ8...BI79

amount : 5
timestamp : 1677628800

TotalStakedTokens: 5

0xIUMS75WM0...65B

amount : 4
timestamp : 1675209600

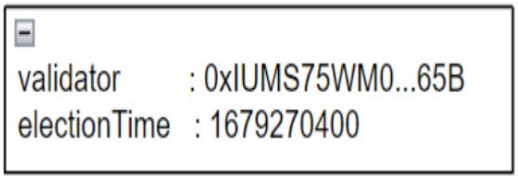
amount : 1
timestamp : 1677628800

TotalStakedTokens: 5

Figure 9: Staked Tokens of two validators

4.3. Choose validator

This can be executed by the admin, in the simulation phase, but in a real scenario, the network will choose a validator every 10 mins as we assumed in the above sections. This takes the winner node address along with the election timestamp. Stores them in the blockchain for further usage. Figure 10 shows the chosen validator to mine the next block.



validator : 0xIUMS75WM0...65B
electionTime : 1679270400

Figure 10: Choose the validator

4.4. Mine

This function can only be called by the validator. This processes the transactions in the pool, compiles them into a block, adds to the chain, resets the runtime variables, and reverts the staked tokens back to the nodes by calculating timestamps for the win and lose scenarios as per the formulae stated in the above sections. The mining done by the chosen validator is shown in Figure 11.

4.5. Simulations

A simple simulation of the proposed formula is done to easily estimate the probability of the validators based on the new methodology which generates the result in a pie chart to understand the result at a glance. The probability of choosing new validators is higher in the case of the new methodology discussed in this paper.

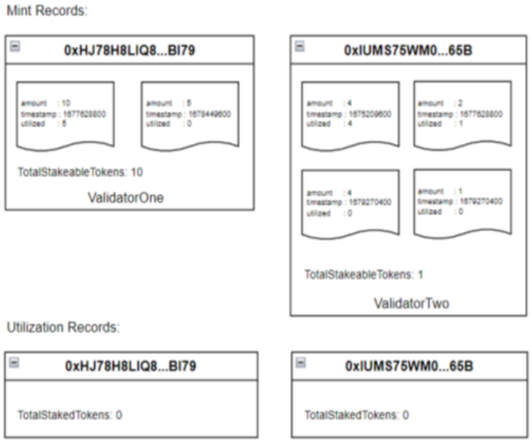


Figure 11: Mining done by the validator

Table 1: Input and output parameters as per new methodology

Input Table		
Election Date (Standard and Epoch Time)	**20-Mar-24**	**1710893365**
	Validator One	**Validator Two**
Minted Date (Assumption)	**1-Mar-24**	**1-Feb-24**
Staked Tokens	**5**	**2**

Output Table		
	Validator One	**Validator Two**
EpochTime	**1709251765**	**1706746165**
AbsoluteDifference	**1641600**	**4147200**
HashPower	**8208000**	**8294400**
RequiredToMatch	**0.989475627**	**1.01641**

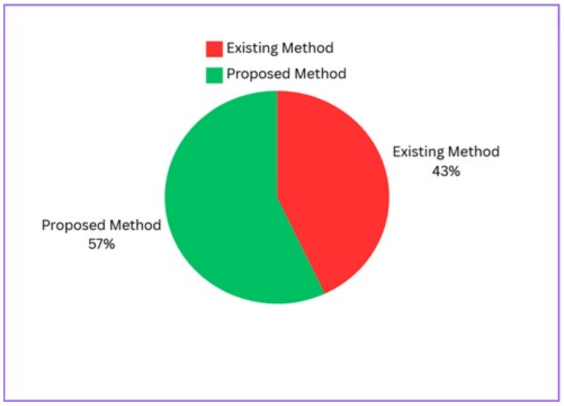


Figure 12: Probability of the validators based on the new methodology

The table 1 shows the assumed inputs and the resulted outputs using the proposed method. The calculations presented in this table is as per the formulae explained in the section 4.

The figure 12 denotes that the proposed method increase the randomness and precision by 14% on the existing strategy.

5. CONCLUSION

The rich-getting-richer syndrome can be mitigated as there exists another parameter called timestamps of staked tokens and they reset on every election. There is no requirement for a validator to wait for 30 days before being able to participate in the next election after winning one. There is no requirement for validator tokens to be at stake for a minimum of 30 days to be able to participate in the election. This approach results in a more randomized and fair selection of validators.
The precision and randomness can be improved with the help of the proposed methodology. These two factors significantly influence the selection of validators, effectively decreasing the "rich-getting-richer" phenomenon and thus satisfying the true decentralization concept.

6. FUTURE SCOPE

The above results are just based on the approach explained in section 3. There are additional approaches in the ideation stage, like considering the actual price of backed tokens and normalizing the parameters used to calculate hash power such that each of them contributed to half of the hash power. They can make the protocol theoretically more robust and fair. Further research on them will be made.

REFERENCES:

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", March 2009, URL: https://bitcoin.org/bitcoin.pdf

[2] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, "Decentralized Applications: The Blockchain-Empowered Software System," in IEEE Access, vol. 6, pp. 53019-53033, 2018, DOI: 10.1109/ACCESS.2018.2870644.

[3] Szabo, N. (1996). Smart contracts: building blocks for digital markets. EXTROPY: The Journal of Transhumanist Thought,(16), 18(2).

[4] Xie Y, Zhang J, Wang H, Liu P, Liu S, Huo T, Duan Y, Dong Z, Lu L, Ye Z, "Applications of Blockchain in the Medical Field: Narrative Review," J Med Internet Res, 2021.

[5] N. Chaudhry and M. M. Yousaf, "Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities," 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), 2018, pp. 54-63, DOI: 10.1109/ICOSST.2018.8632190.

[6] S. M. S. Saad, R. Z. R. M. Radzi and S. H. Othman, "Comparative Analysis of the Blockchain Consensus Algorithm Between Proof of Stake and Delegated Proof of Stake," 2021 International Conference on Data Science and Its Applications (ICoDSA), 2021, pp. 175-180, DOI: 10.1109/ICoDSA53588.2021.9617549.

[7] W. Wang et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," IEEE Access, 2019.

[8] Vasin, P, "Blackcoin's proof-of-stake protocol v2", 2014, URL: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf, volume=71

[9] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, E. Dutkiewicz, "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities," in IEEE Access, 2019.

[10] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism," in IEEE Access, vol. 7, pp. 118541-118555, 2019, DOI: 10.1109/ACCESS.2019.2935149.

[11] R. Smith. (2019). Proof of Burn | Consensus Through Coin Destruction, Article Published by Coin Central. [Online]. Available:https://coincentral.com/proof-of-burn

[12] I Bentov, C Lee, A Mizrahi, M Rosenfeld, "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract]y.," SIGMETRICS Perform. Eval. Rev., 2014.

[13] Peter Compare. What is Proof of Weight, a Web Article Published by Coincodex. Accessed: 2019. [Online]. Available: https://coincodex.com/article/2617/what-is-proof-of-weight/.

[14] A. Pal, K. Kant, "DC-PoET: Proof-of-Elapsed-Time Consensus with Distributed Coordination for Blockchain Networks," IFIP Networking Conference (IFIP Networking), 2021.

[15] Sayeed S, Marco-Gisbert H. "Proof of Adjourn (PoAj): A Novel Approach to Mitigate Blockchain Attacks". Applied Sciences. 2020; 10(18):6607, https://doi.org/10.3390/app10186607.

[16] V. N. C. P. L. E. Z. Igor and M. Coelho, ‘‘Delegated Byzantine fault tolerance: Technical details, challenges and perspectives,’’ NEO, Shanghai, China, Tech. Rep., Mar. 2019, sec. 8. [Online]. Available:https://neoresearch.io/assets/yellowpaper/yellow_paper.pdf.

[17] A Li, X Wei, Z He, "Robust Proof of Stake: A New Consensus Protocol for Sustainable Blockchain Systems," Sustainability, MDPI, 2020.

[18] M. Saad, Z. Qin, K. Ren, D. Nyang and D. Mohaisen, "e-PoS: Making Proof-of-Stake Decentralized and Fair," in IEEE Transactions on Parallel and Distributed Systems, 2021.

[19] Thin, Wai & Dong, Naipeng & Bai, Guangdong & Dong, Jin. (2018). "Formal Analysis of a Proof-of-Stake Blockchain". 197-200.10.1109/ICECCS2018.2018.00031.

[20] Y Shifferaw, S Lemma, "Limitations of proof of stake algorithm in Blockchain: A review," Journal of EEA, 2021.

[21] "Proof of Stake versus Proof of Work White Paper", September 13, 2015, BitFury group, version 1.0, URL:https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf.

[22] P. Rajitha, D. Ramya, "Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain," in Proceedings of the Third International Conference on Intelligent Communication

Technologies and Virtual Mobile Networks (ICICV), 2021.

[23] Anjaneyulu Endurthi, Akhil Khare, "Two-Tiered Consensus Mechanism Based on Proof of Work and Proof of Stake," 9th International Conference on Computing for Sustainable Global Development, 2022.

[24] H. Xiong, M. Chen, C. Wu, Y. Zhao, W. Yi, "Research on Progress of Blockchain Consensus Algorithm: A Review on Recent Progress of Blockchain Consensus Algorithms," Future Internet, 2022.

[25] V Buterin, "Ethereum White paper", Journal of Information science, 39(1), pp 101-112, 2013, doi:10.1177/0165551512470051.

[26] Buterin, V., et al.: A next-generation smart contract and decentralized application platform. White Paper (2014).

[27] Dannen, C.: Introducing Ethereum and Solidity. Springer, Berkeley (2017).

[28] J. Kwon and E. Buchman, "Cosmos whitepaper," 2019. [Online]. Available: https://cosmos.network/cosmos-whitepaper.pdf.

[29] Gavin Wood, Polkadot: Vision for a heterogeneous multi-chain framework, 2016.

[30] Goodman, L. Tezos—A Self-Amending Crypto-Ledger White Paper. 2014. Available online: https://academy.bit2me.com/wp-content/uploads/2021/04/tezos-whitepaper.pdf (accessed on 28 July 2021).

[31] Allombert, Victor & Bourgoin, Mathias & Tesson, Julien. (2019). Introduction to the Tezos Blockchain.

[32] Leonard Lys and Sebastien Forestier and Damir Vodenicarevic and Adrien Laversanne-Finot, 2023, Defending against the nothing-at-stake problem in multi-threaded blockchains.

[33] Anjaneyulu Endurthi, H. N. Gurram, H. Mohamad, A. Sriram and, "A Strategy to Improvise Coin-age Selection in the Proof of Stake Consensus Algorithm," 2023 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 2023, pp. 1-4, doi: 10.23919/SoftCOM58365.2023.10271652.