I. J. Computer Network and Information Security, **2025, 6, 84-97**
Published Online on December 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2025.06.06

Scalable-pos: Towards Decentralized and Efficient Energy Saving Consensus in Blockchain

Anupama B. S.*
Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Visvesvaraya Technological University, Belagavi-590018, Karnataka, India
E-mail: anupamabs@sit.ac.in
ORCID iD: https://orcid.org/0009-0005-3973-7338
*Corresponding author

Sunitha N. R.
Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Visvesvaraya Technological University, Belagavi-590018, Karnataka, India
E-mail: nrsunitha@sit.ac.in
ORCID iD: https://orcid.org/0000-0003-4990-1689

G. S. Thejas
Department of Computer Science and Electrical Engineering, Tarleton State University, Texas A&M University System, TX, USA
E-mail: sadashiva@tarleton.edu
ORCID iD: https://orcid.org/0000-0001-9606-0128

Received: 10 June 2025; Revised: 21 August 2025; Accepted: 29 September 2025; Published: 08 December 2025

Abstract: Blockchain has become peer-to-peer immutable distributed ledger technology network, and its consensus protocol is essential to the management of decentralized data. The consensus algorithm, at core of blockchain technology (BCT), has direct impact on blockchain's security, stability, decentralization, and many other crucial features. A key problem in development of blockchain applications is selecting the right consensus algorithm for various scenarios. Ensuring scalability is the most significant drawback of BCT. The industry has been rejuvenated and new architectures have been sparked by the usage of consensus protocols for blockchains(BC). Researchers analyzed shortcomings of proof of work (PoW) consensus process and subsequently, alternative protocols like proof of stake (PoS) arose. PoS, together with other improvements, lowers the unimaginably high energy usage of PoW, making it protocol of time. In PoS, only the user with highest stake becomes the validator. To overcome this, we propose Scalable Proof of Stake (SPoS), a novel consensus protocol, which is an enhancement of PoS protocol. In the proposed algorithm, each stakeholder based on the stake gets a chance to become the validator and can mine blocks in the blockchain. Clustering of the stakeholders is done using mean shift algorithm. Each cluster gets a different number of blocks to mine in BC. Cluster with highest stake will get a greater number of blocks to mine when compared to other groups and the cluster with the least stake gets least number of blocks to mine when compared to other groups. To mine the blocks, validator is chosen based on the cluster in which he is present. Fair mining is ensured for all stakeholders based on number of stakes. Mining is distributed among all the stakeholders. Since the validators are chosen fast, the transaction rate is high in the network. Validators in PoS are selected according to the quantity of cryptocurrency they stake. More stakeholders will get chance of validating blocks and receiving rewards. Over time, this reduces fairness and decentralization by concentrating on wealth and power. This is addressed in SPoS using clustering-based validator assignment.

Index Terms: Blockchain, Consensus Protocol, Decentralization, Proof of Stake, Scalability.

1. Introduction

BC are distributed, shared databases that do not require single point of control to securely retain digital footprints. Smart contracts can be integrated with blockchains to create transparent, secure, and unchangeable systems that produce distinctive outcomes. Furthermore, BC is a decentralized ledger that uses cryptographic programs to record user activity across many users without the need for single control center. Blocks to be added to chain is validated by all participating users, and a consensus process makes sure that everyone agrees on a particular sequence for blocks to be added.

Participants' stake is more important to the Proof-of-Stake (PoS) than their processing power. In Proof of Stake (PoS), miners are chosen according to stake, or balance, and network adjusts to suit their opinions. Coins are created during the cryptocurrency's launch in most PoS-based cryptocurrencies. As a result, miners receive no rewards. Rather, miners make money by keeping transaction fees. In PoS, miners are chosen by a procedure analogous to an auction, in which bidders compete for the next block, with the highest bidder winning the auction.

1.1. Consensus Protocol

One of a BC's key technologies, consensus algorithm [1,2],significantly affects performance metrics including transaction throughput, latency, and rate at which blocks are generated in BC systems. There are many kinds of consensus processes in recent years. Consensus methods generally fall into 3 categories: PoW [3], which is based on competition for computing power; PoS [4], which is based on Coin Days and proof of credit (PoC) [5], which is based on credit. Specifically, improved consensus method evolved from PoS called delegated proof of stake (DPoS) [6] has become common algorithm. It uses voting to select k representative nodes, and after each election round, these k nodes alternate in producing blocks. The DPoS algorithm, in contrast to PoW and PoS, selects representative nodes to generate blocks [7], which lowers waiting time needed to verify transaction and raises rate of block generation. Researchers have suggested better techniques for DPoS [8,9]. It is currently utilized in several industries, including supply chain management and digital currency. For instance, DPoS is used by BitShares to create decentralized trading platform and by EOS to create decentralized application platform.

Since larger nodes can easily overwhelm smaller ones, traditional PoS inhibits decentralization. This is because chosen delegates are essential to PoS systems' ability to verify transactions and preserve network integrity. Smaller nodes find it more challenging to take part in the consensus process since larger nodes are better equipped to manage the delegation selection procedure. As a result, PoS networks can eventually become less decentralized, which is contrary to one of the core principles of blockchain technology. Another prominent criticism of PoS is its lack of scalability. This is due to the fact that PoS systems perform worse than PoW systems when managing many transactions. Therefore, compared to blockchains that employ PoW, those that use PoS may have higher costs and slower transaction speeds. One of the primary criticisms of PoS is the potential for power concentration. A situation in which one party has complete control over the blockchain network could arise from that entity controlling all these validators. The decentralization principle that underpins blockchain technology would be violated by this. Because traditional hard computing techniques are less decentralized, less robust, less scalable, and inefficient, they might not be able to solve these issues effectively. Transaction processing speeds are extremely slow, and efficient fair mining might not be the best option. This leads to the selection of validators inefficiently. We suggested the Scalable PoS technique, which is a decentralized, robust, scalable, and effective fair mining algorithm, to address the shortcomings of the conventional PoS consensus process.

1.2. Outline

Rest of paper is organized as follows: Section 2 examines literature work. Section 3 talks about Proof of Stake. Section 4 shows working of proposed algorithm. Section 5 presents analysis of result. Finally, concludes in Section 6.

2. Literature Review

PoW is first blockchain consensus protocol. Bitcoin uses this protocol to achieve consensus, which introduces computing power competition between distributed nodes to ensure consistency of data and security of consensus. Bitcoin's system generates new transactions constantly, and nodes are responsible for putting legitimate transactions into blocks. Block header should contain six parts: version number, previous block hash value, Merkle root, timestamp, difficulty target noise and random number. The PoW protocol is used primarily in digital currencies like Dogecoin[10] and Litecoin[11].

Limitations of PoW: PoW based blockchain applications' energy inefficiency has drawn a lot of focus in [12–15]. Bahri and Girdzijauskas [12]examined how much energy Bitcoin used in order to run its fundamental consensus mechanism. According to their estimates, the average annual use of Bitcoin is 39.5 TWh of electricity. When Bitcoin began to grow, Dwyer and Malone [13]saw that miners were using lot of electricity and predicted that this would become significant issue. Harald Vranken [16]resource analysed the most popular PoW-based blockchain applications in order to investigate the sustainability of blockchains and Bitcoin. In addition, his research links the endogenous PoW needs to the rising energy footprint of the Bitcoin cryptocurrency.

Limitations of PoS: Even though PoS attempts to alleviate PoW's [17–19] increasing energy-related issues it brings unfairness into the system and is open to multiple attacks. There have been reports on the "rich get richer" tendency[20], [21] in mining. In proof-of-stake, the baseline stakes divide the network so that number of peers that are above baseline always receives fee rewards. As a result, both the baseline stake threshold and division margins between wealthier nodes and remaining nodes in network continue to rise. This PoS constraint was noted by Zheng et al.[21], who also emphasised the necessity for new PoS method. Kiayias et al. [22] employed PoW based theoretical model put forth by Garay et al. [23] to conduct a rigorous examination of PoS-based blockchains in order to achieve that goal. They formally outlined the required security characteristics for a proof-of-stake blockchain system, and they then used those characteristics to introduce the "Ouroboros" paradigm. To discourage selfish mining attacks and encourage PoS-based systems, Ouroboros employs a special rewards structure. The authors of Ouroboros inject randomization into miner selection through the use of a coin-flipping mechanism. Despite its advantages, random selection may compromise fairness. Each stakeholder's balance needs to be higher than the baseline stake in order to guarantee fairness. The security of random selection can be jeopardised because a miner's balance is frequently less than the baseline stake. Because random mining selection circumvents the baseline stake's security requirements, it may therefore be detrimental to the e-PoS architecture.

Similar to this, Diant et al. [24] introduced SNOW WHITE, PoS based protocol variation that enables safe use of PoS in permissionless BC systems. SNOW WHITE uses a random miner selection process to accomplish decentralisation, which is akin to the work of [22]. To create the illusion of randomness, SNOWWHITE, extension of "Sleepy Consensus" [25], adds dependency between block headers in place of coin-flipping technique in [24]. Lastly, Chen et al.'s work [26] on Algorand, which employs message-passing Byzantine Agreement to reach agreement in large-scale distributed networks, remains noteworthy. It is presently being implemented in a few blockchain systems and uses considerably less energy to run.

DPoS and Supernode PoS (SPoS) are two more noteworthy PoS-based protocols. The network users in (DPoS) cast votes to choose a group of witnesses who mine blocks [27]. In SPoS, supernodes are chosen to mine blocks, which is continuation of DPoS [28]. In contrast to the DPoS, SPoS ensures optimal data storage and a consistent inter-arrival block time. Before mining a block, miners pledge their stakes in both protocols. Miners lose their investments if they misbehave. Main issue with this strategy is that a miner can simply cheat and violate the fairness property if the incentive for misbehaviour is higher than the stake. In order to deter malicious behaviour, no system ties stakes to monetary rewards.

The PoS protocol is well substitute for PoW that addresses PoW's drawbacks and accomplishes comparable goals[29]. A candidate miner must stake his balance in order to be chosen to mine the subsequent anticipated block in PoS. First cryptocurrency to use PoS for block mining was Peercoin, which was introduced in 2012 [30]. Later, more PoS-based cryptocurrencies were introduced, such as Nxt and BlackCoin. The terms "randomised block selection" and "coin age based selection" refer to two widely used miner selection methods. The candidate with lowest hash value and size of their stake are combined in randomised block selection process to choose the miner for the subsequent block. An auction procedure is used in coin age based selection process to choose candidate miners.

Despite being energy-efficient, PoS causes centralization [31,32]. When using randomised block selection, a random candidate is chosen rather than the deserving candidates with large stakes. A wealthy candidate has the ability to win every auction and increase in wealth in open stakes auction and age based selection [31], [33]. This leads to a network skew, which brings upon the decentralisation of the network, which is normally assumed in a blockchain application. Additionally, the balance of candidate miners is revealed via publicly disclosed stakes, jeopardising their privacy and anonymity. Furthermore, using PoS, it is simple to create new block and split off the main chain because anyone may do so with little difficulty. An attacker of this kind can use network churn and latency to determine which nodes are trailing the main chain and divide them using his customised blockchain [34,35].

Hybrid Schemes: Hybrid techniques are used to combine advantages of these consensus schemes while lowering the attack surface in order to solve their drawbacks. TwinsCoin is a safe and expandable hybrid blockchain protocol proposed by Duong et al.,[36]. Proof-of-Activity (PoA), a hybrid blockchain system introduced by Bentov et al.[37], improves blockchain defense mechanisms with little penalty on network traffic and storage capacity. To protect blockchains from majority and centralization threats, some noteworthy initiatives are made [37, 38], [17]. In spite of these admirable attempts, a workable solution that can be implemented on current cryptocurrencies to facilitate their seamless transition to proof of stake is still required.

We expect an update to the current consensus schemes to enhance decentralisation and equity, considering the aforementioned constraints. Naturally, we anticipate a PoS variation or an energy efficient model independent of computationally demanding mining. Protocol should provide mining possibilities to larger range of stakers to promote decentralisation. Preventing fraudulent actions and compensating impacted parties fairly in the event of an attack are essential components of a fair protocol. Protocol must provide reward system that encourages honest mining while maintaining fairness. With this in mind, we proceed to construct an algorithm that tackles these issues and offers framework for further uses.

Table 1. Comparison of consensus protocols

Papers	Parameters
[39]	Energy-saving, robustness
[40]	Tolerated power of adversary, capitalization market, TPS, energy saving
[41]	Gini index, request satisfied ratio, coin price index
[42]	Computing power distribution, energy saving
Proposed Work	Decentralization, Robustness, Efficient energy saving, TPS, fairness

2.1. POS

POS was first introduced in Peercoin and has become second most popular mechanism in world. Consensus in POS system is based on each node's stake. The Peercoin unit of POS is coin day, which is amount of money multiplied by time it has been held. In peer-to-peer network, each node adds its block to chain according to its fortune. A validator with more coin-days will be more likely to create new blocks. Validators need two inputs to create a new block: kernels and stakes. Input that leads to particular target hash is called a kernel input. The stake input is number of coin days validator must spend to create block. More coin days validator spends, faster hashing process. Transactions collected by validator are contained in the new block.

A maximum coin owner is selected at random by the proof of stake process to validate a transaction. The owner is also able to make a block for the same coin. Comparatively speaking, this technique uses less energy and requires a shorter transaction time. PoS has addressed the problem of significant energy resource waste. Moreover, PoS-based systems authorize transactions significantly faster than PoW based systems and are far more scalable. Scalability is the ability of a system to change parameters or modify its consensus mechanism to accomplish higher transactions per second (TPS) than certain existing systems.

In traditional PoS, PoS prevents decentralization since bigger nodes can simply overwhelm smaller ones. This is because PoS systems depend on selected delegates to authenticate transactions and keep network up to date. Smaller nodes find it more challenging to take part in the consensus process since larger nodes can more easily manage the delegation selection process. Because of this, PoS networks may eventually become less decentralized, which is contrary to one of key principles of BC technology.

PoS is frequently criticized for its inadequate scalability as well. This is due to fact that PoS systems perform less effectively than PoW systems while managing a high volume of transactions. Therefore, compared to blockchains that employ PoW, those that use PoS may see lesser transaction rates and higher costs.

Possibility of power centralization is one of main objections levelled against PoS. This is so because PoS systems depend on limited group of "validators" or "delegates" to authorize transactions and uphold network. A scenario where a single entity controls all these validators could result in that entity having total control over BC network. This would go against decentralization idea that is the basis of blockchain technology.

Finding a solution to these problems using traditional hard computing algorithms may not produce efficient results because they are less decentralized, less robust, low scalable and inefficient. The processing speed of transactions is very low, and efficient fair mining may not be optimal. This results in inefficient validator selection.

To overcome drawbacks of traditional PoS mechanism, we proposed Scalable PoS technique in which the algorithm is decentralized, robust, scalable and efficient fair mining is achieved.

2.2. Contribution

We propose a novel consensus protocol which is an enhancement of the POS protocol in BCT:

- We propose a Scalable PoS (S-PoS) consensus mechanism that permits fair, decentralized and energy efficient mining in blockchain systems to overcome the drawbacks of PoS.
- Scalability is examined by mining the blocks for different number of stakeholders.
- Performance analysis is done for blocks mined and average time for mining in different blockchains like Ethereum and Cardano.

3. Methodology

A new Scalable POS is proposed which achieves decentralization and fairness by enabling each stakeholder to become the validator to mine the blocks in the BC. Figure 1 illustrates the working of proposed algorithm and flowchart of proposed algorithm is shown in figure 2.

3.1. Architecture of Proposed Algorithm

Elements of proposed algorithms are

Nodes: Users in the blockchain network. A node can become validator by staking his coins in the network.

Staker (Stakeholder): A person who invests his coins in the network. Staker becomes validator only after staking his coins in network.

Stakes: The amount invested by the staker.

Validator: Staker who can validate and create blocks in BC.

Blockchain: It is distributed, decentralized digital ledger of transactions.

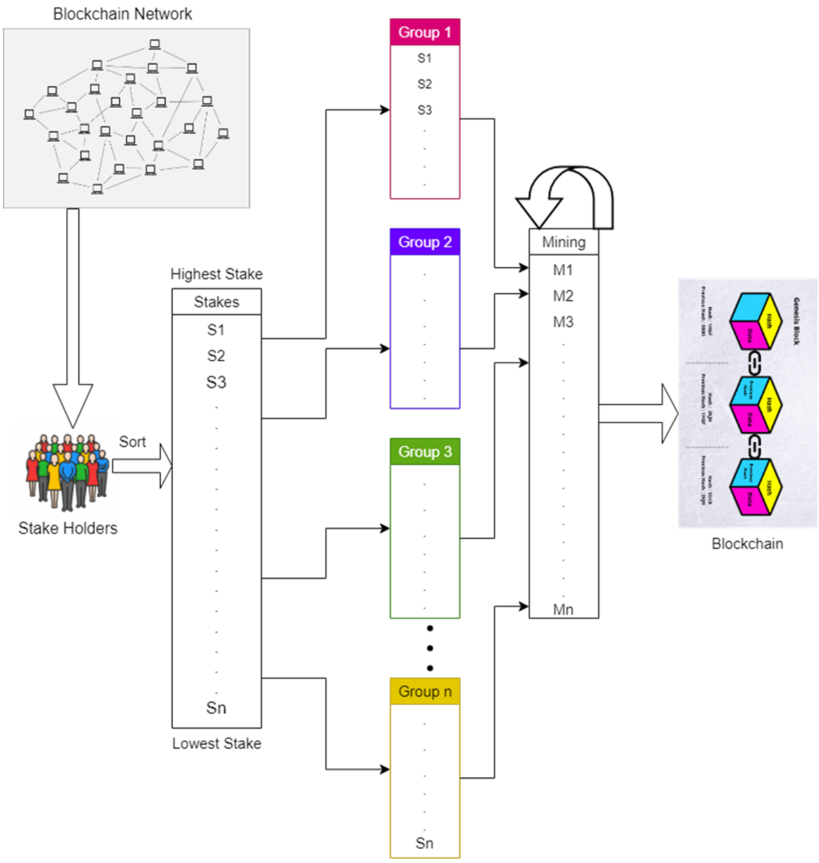

Fig.1. Working of proposed algorithm

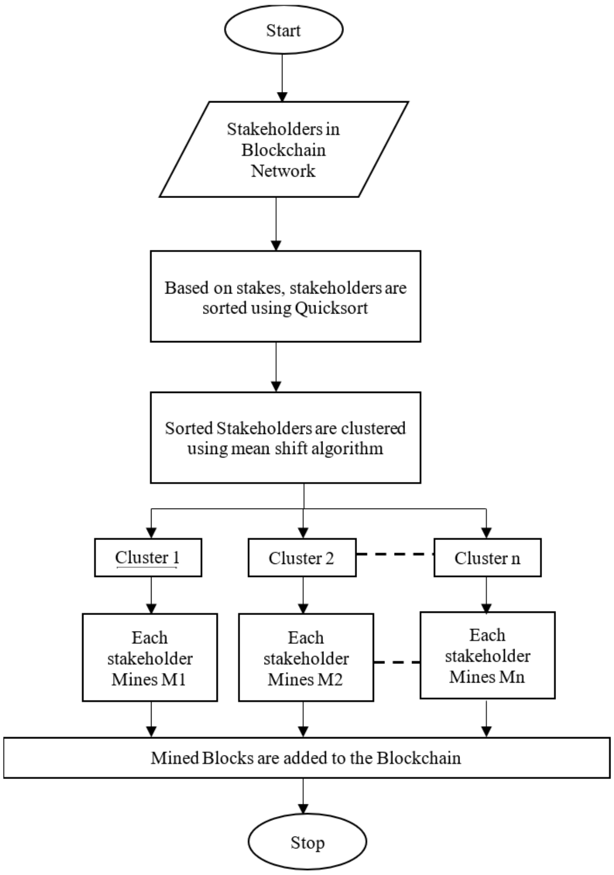
Start
Stakeholders in Blockchain Network
Based on stakes, stakeholders are sorted using Quicksort
Sorted Stakeholders are clustered using mean shift algorithm
Cluster 1
Cluster 2
Cluster n
Each stakeholder Mines M1
Each stakeholder Mines M2
Each stakeholder Mines Mn
Mined Blocks are added to the Blockchain
Stop

Fig.2. Flowchart of proposed algorithm

To stake the coins each user should join the network. Once the user joins the network then user can stake the coins to become the validator for mining the blocks. If the user wants to become the validator, then user stakes the coins. Once coins are staked then it will be locked in the network. Stakeholders are sorted using quick sort algorithm. The stakeholder with highest stake will be the first and the stakeholder with least stake will be the last in the sorted list of stakeholders. The sorted list of stakeholders is grouped using Mean Shift algorithm. The stakeholder with highest stake will be in first group and the stakeholder with least stake will be in last group. Each stakeholder in the network is given a chance to become the validator based on the group in which they are present in a round robin fashion. First group members can mine M1 blocks, second group members can mine M2 and last group members can mine Mn blocks. M1, M2,. Mn are number of blocks to be mined by stakeholders. Mining is done in two rounds. In the first round, except the last group each group stakers mines (blocks_len – multiplier) blocks starting from group G1 which consists of stakers with highest stakes. In the second round, each group stakers mines multiplier blocks starting from group G1 till last group. Each staker gets a chance to become a validator and can mine the blocks based on number of stakes.

3.2. Implementation of Proposed Algorithm

The proposed consensus is divided into 4 phases.

Phase 1: Staking Coins
Phase 2: Sorting
Phase 3: Clustering
Phase 4: Mining

Phase 1: Staking the Coins

To stake the coins each user should join the network. Once the user joins the network then user can stake the coins to become the validator for mining the blocks. If the user wants to become the validator, then user stakes the coins. Average stake is calculated by dividing total stakes of all nodes by number of nodes in blockchain. If the staked coins of a node are greater than the 32 Ethers, then that node is added as a stakeholder. Once coins are staked then it will be locked in the network.

Algorithm: Staking the coins

```
for each node i in blockchain_nodes:
    if i. stake > 32
        add i as stakeholder.
    else
        cannot add i as stakeholder
```

Phase 2: Sorting

The users who staked their coins are sorted in the decreasing order of the stakes. The stakeholder with highest stake will be the first and the stakeholder with least stake will be the last in the sorted list of stakeholders. By choosing a pivot element p_Element, stakes array arr can be subdivided into smaller stake arrays. The stakes array arr should be divided with the p_Element positioned so that elements larger than p_Element are on right side of p_Element and elements less than p_Element are kept on left. Left and right subarrays are divided using similar technique. This process is repeated until each subarray contains only one element. At this stage, elements have already been resolved. Finally, pieces are combined to make a sorted array.

Algorithm: To Sort the Stakes

```
sort (arr, lm_Index, rm_Index)
  if (lm_Index < rm_Index)
    p_Index = partition (arr, lm_Index, rm_Index)
    sort (arr, lm_Index, p_Index – 1)
    sort (arr, p_Index, rm_Index)

partition (arr, lm_Index, rm_Index)
   set rm_Index as p_Index
   Index = lm_Index – 1
   for I = lm_Index + 1 to rm_Index
   if element[i] < p_Element
      swap element[i] and element [Index]
      Index++
   swap p_Element and element [Index+1]
```

```
return Index + 1
```

Phase 3: Clustering

The sorted list of stakeholders (SH) is grouped according to the stakes of stakeholders using meanshift clustering algorithm. The stakeholder with the highest stake will be given first priority when compared to the stakeholder with the least stake in the group. The dataset {si} consisting of SH and stakes is given as input to the mean shift clustering algorithm. Considering a dataset {si} comprising points in m-dimensional space, which was selected from a broader population, we have selected kernel ker with bandwidth parameter of b. Following kernel density estimator for density function of full population is obtained by combining these data with kernel function.

$$f_{ker}(s) = \frac{1}{nb^m}\sum_{i=1}^{n} ker\left(\frac{s - s_i}{b}\right)$$

Here, the two requirements listed below must be met by the kernel function:

$$\int ker(s)\,ds = 1 \tag{1}$$

$$ker(s) = ker(|s|) \text{ for all values of s} \tag{2}$$

Equation (1) must be met to ensure that the estimate is normalized. Equation (2) is related to symmetry of space. The kernel functions that satisfy equation (1) and (2) are

$$Flat\ /\ Uniform\ \text{ker}\ (s)\ = \frac{1}{2}\begin{cases} 1 & -1 \le |s| \le 1 \\ 0 & else \end{cases}$$

$$Gaussian = \text{ker}(s) = \frac{1}{(2\pi)^{\frac{m}{2}}} e^{\frac{-1}{2}|s|^2}$$

The reshape function will reshape input dataset into a single array of column. The bandwidth will be estimated automatically. When bin_seeding=True, the data is binned in order to select the first cluster centers. After meanshift model fitting, cluster_centers return coordinates of cluster center and labels return unique labels assigned to each data point. Cluster count is stored in n_clusters. Dictionary is initialized using cluster_members in order to store cluster members of clusters. Data points are then iterated through, with each point being assigned to the appropriate cluster according to its label. Lastly, for simplicity, it turns the lists of cluster members into NumPy arrays.

Algorithm: Clustering Stakes

```
S1 = np. reshape (dataset, (-1, 1))
MS = MeanShift (bandwidth=None, bin_seeding=True)
MS.fit (S1)
labels = MS. labels_
cluster_centers = MS. cluster_centers_

labels_unique = np. unique(labels)
n_clusters_ = len(labels_unique)
labels_unique = np. unique(labels)
cluster_members = {label: [] for label in labels_unique}

for i, label in enumerate(labels):
  cluster_members[label]. append(S1[i])
for label in labels_unique:
  cluster_members[label]=np. array(cluster_members[label])
for label, members in cluster_members. items ( ):
  print ("Cluster {label}: {len(members)} members")
  print (members)
```

Phase 4: Mining

Each stakeholder in the network is given a chance to become the validator based on group in which they are present. Groups are divided based on stakes. Stakers with the highest stakes will be in first group and the stakers with the least stakes will be in last group. First group members can mine M1 blocks, second group members can mine M2 and last group members can mine Mn blocks. M1, M2…...Mn are number of blocks to be mined by stakeholders in clusters G1, G2……. Gn respectively. Where M1 > M2 > M3 > …………. > Mn. Clusters number is stored in groups_number and clusters are given as input to mining. Number of stakers in each group is stored in groups_length. Initially genesis block is mined. Loop is iterated to find number of blocks to be mined by each group until total_blocks_to_be_mined is greater than blocks_mined_in_different_blockchain. Number of blocks to be mined by each group is done in two rounds. In first round, except the last group each group stakers mines (blocks_len – multiplier) blocks starting from group G1 which consists of stakers with highest stakes. In the second round, each group stakers mines multiplier blocks starting from group G1 till last group. Each staker gets a chance to become a validator and can mine the blocks based on number of stakes.

Algorithm: Mining

```
groups = [G1, G2, G3……...Gn] where Gi = [ S1, S2…...]
groups_number = [n…….4,3,2,1]
groups_length = [L1, L2……]
multiplier = 0
total_blocks_to_be_mined = 1

while (total_blocks_to_be_mined < blocks_mined_in_different_blockchain)
    multiplier = multiplier + 1
    for groupnum in groups_number:
        blocks_to_be_mined = groupnum * multiplier
    blocks_to_be_mined = [M1, M2, M3…...]
    for grouplen in groups_length, for blocks_len in blocks_to_be_mined:
        total_blocks_to_be_mined + = (L1*M1) + (L2*M2) + …………

for group in groups, for blocks_len in blocks_to_be_mined:
    for staker in group:
        for block_mined in range (blocks_len – multiplier):
            mine_block(staker)

for group in groups:
    for staker in group:
        for block_mined in range(multiplier)
            mine_block(staker)
```

Mean-shift clustering automatically calculates number of clusters based on data distribution, in contrast to K-means, which necessitates defining the number of clusters k beforehand. This is especially helpful in dynamic or decentralized settings, such as validator pools, where the ideal number of groups is unpredictable and subject to change over time. The spherical and equal-sized cluster assumption made by K-means may not accurately represent the distribution of validators in practice More organic groupings result from mean-shift's ability to detect groups of arbitrary forms without making such assumptions. Dense regions in the data space are identified using mean-shift. Since validators with more similar performance, conduct, etc. are clustered together, bias or concentration of influence among high-density zones is lessened, which is in line with fairness aims. When determining centroids, mean-shift is typically more resilient to outliers than K-means, which can be significantly impacted by distant points. This prevents validators who exhibit infrequent but acceptable conduct from being unfairly penalized or excluded. The non-parametric nature of mean-shift enables it to adjust to changes more gracefully and without the need for manual retuning, as validator behavior and metrics may change over time.

4. Results and Discussion

4.1. Comparing Features of Consensus Protocols

Robustness: Blockchain systems are also vulnerable to variety of cyberattacks, including random number attacks and distributed autonomous organisations (DAOs)[43], which have emerged as major threats to steady and long-term growth of blockchain systems. Due to limited number of mining pools, PoW systems (like Bitcoin) are becoming more and more centralised, which increases the system's vulnerability to a 51% attack. Therefore, as we showed in Table 2, PoW systems frequently have low robustness. PoS systems are vulnerable to Nothing-at-Stake and coin age accumulation attacks. As a result, PoS is highly vulnerable to these two assaults. To strengthen the blockchain system against such attacks, we proposed Robust SPoS. There is essentially no chance of a coin age accumulation attack or a network-wide denial-of-service attack in the system since SPoS employs number of coins rather than coin age to determine mining opportunities. SPoS is robust against the above two attacks.

Efficient Energy saving: Rapid economic growth leads to high levels of energy consumption and carbon dioxide emissions, which have dramatically altered global climate and had a negative impact on human living conditions. As result, it is essential to create a distributed economy system that emits little carbon dioxide and conserves energy[39]. Intermediaries can be eliminated and processes can be streamlined with blockchain technology. Transactions may become faster and more effective as a result. PoW systems are energy-intensive and unsustainable because miners need lot of energy to compete for mining chances by using lot of mining devices. Hence efficient energy saving is low in PoW. PoS systems are far more energy efficient and long-lasting than PoW systems since mining competition is based on number of coins stored and age of coins. Based on number of coins, miners compete for mining opportunities in SPoS. Similar to PoS, SPoS has low power usage without need for mining equipment. Therefore, in terms of energy savings, PoS and SPoS both outperform PoW.

Transaction per Second: TPS is a crucial metric for assessing a financial system's effectiveness since it shows how many transactions the system completes each second[21]. VISA can process about 1700 TPS on average. On other hand, popular blockchain systems like Ethereum and Bitcoin are limited to less than 30 transactions per second[44], which means that they cannot handle the large number of transactions that occur in real life. Since the SPoS protocol is PoS-based and does not require a coin age selection and clearing process, it is highly probable that it will operate faster than PoS.

Decentralization: In order to attain decentralisation and mitigate the skews inherent in traditional Proof of Stake (PoS), SPoS enables all stakeholders to mine blocks on the blockchain according to their respective stake amounts and group memberships. Due to a limited number of mining pools, PoW systems (like Bitcoin) are becoming more and more centralised, which increases the system's vulnerability to a 51% attack. In PoS, the staker with highest stake will be the validator always so, decentralization is low. In SPOS, each staker will become the validator so decentralization is high.

Fairness: In order to attain equity and mitigate the skews inherent in traditional Proof of Stake (PoS), SPoS enables all stakeholders to mine blocks on the blockchain according to their respective stake amounts and group memberships. Because group 1 stakers have staked more coins than other groups, they will mine more blocks than other groups and, as a result, receive higher rewards. Mining becomes fair since any staker, regardless of the group, will mine the blocks and receive a reward in return. In PoW, the node with good hardware requirements will become the miner and in PoS, the node with highest stake will always become the validator so, fairness is low. In SPoS, each staker will become the validator so, fairness is high.

Table 2. Comparison of features in blockchain systems

Features	PoW	PoS	SPoS
Robustness	Low	High	High
Efficient energy saving	Low	High	High
TPS	3-7	10-30	3530
Decentralization	Low	Low	High
Fairness	Low	Low	High
Hash Value/ Miner Selection	Depends on computing power	Depends on Stake and coin age	Depends on the amount of stake

PoS systems are vulnerable to Nothing-at-Stake and coin age accumulation attacks. As a result, PoS is highly vulnerable to these two attacks, as seen in Table 3. There is virtually no chance of a Nothing-at-Stake assault or a coin age accumulation attack in the system because SPoS uses quantity of coins rather than coin age to determine mining possibilities. Since PoW lacks the notion of stake, it is naturally impervious to these PoS attacks. Since a 51% attack would have a negative payoff, sensible nodes in PoS and SPoS systems will not carry it out. Therefore, we propose that there is little chance of a 51% assault in PoS and SPoS systems.

Table 3. Comparison of attacks in blockchain systems

Attacks	PoW	PoS	SPoS
Coin age accumulation	NA	High	Low
51% attack	High	Low	Low
Nothing-at-Stake	NA	High	Low

4.2. Simulation Results

Simulation results are taken for upto 5000 stakers in Ethereum and Cardano using SPoS consensus protocol. The table 4 illustrates number of clusters formed, blocks mined and time taken in milliseconds in Ethereum and Cardano for different number of stakers.

Table 4. Simulation in blockchain systems

Number of Stakers	Clusters Formed	Ethereum		Cardano	
		Blocks mined	Time taken (ms)	Blocks mined	Time taken (ms)
1000	5	27751	906.21	36076	952.93
2000	4	22706	1062.27	31788	1093.49
3000	5	27037	1234.06	36049	1312.39
4000	4	27205	1515.24	36273	1640.24
5000	7	38345	1733.97	57517	1999.56

Currently in Bitcoin PoW for mining a block it takes around 10 minutes. For one hour Bitcoin will mine around 6 blocks. In Ethereum PoS to mine a block it takes around 15 seconds. For one-hour Ethereum will mine around 240 blocks. In Cardano PoS to mine a block it takes around 20 seconds. For one hour Cardano will mine around 180 blocks. Similarly, in SPoS simulation to mine a block it takes 2.83 milli seconds. For one-hour SPoS will mine around 1272085 blocks since it is network independent simulation. Blocks mined per hour in Bitcoin, Ethereum, Cardano and SPoS is shown in Table 5. Bitcoin, Ethereum and Cardano follows single validator architecture whereas SPoS is a multiple validator architecture.

Table 5. Blocks mined in blockchain systems

	PoW (Bitcoin)	PoS (Ethereum)	PoS (Cardano)	SPoS
Blocks mined per Hour	6	240	180	1272085

Figure 3 shows clusters formed for 1000 stakers and 5000 stakers. In 1000 stakers, clusters formed are 5 and in 5000 stakers, clusters formed are 7. Figure 4 illustrates clusters formed for different stakers. Figure 5 illustrates blocks mined in Ethereum and Cardano. Figure 6 time taken in milliseconds for mining in Ethereum and Cardano. Number of clusters formed and number of cluster members in each cluster for different stakers are shown in figure 7. Table 6 illustrates number of Clusters formed, cluster members, average and median cluster sizes for different stakers. Figure 8 shows the average and median cluster sizes for different stakers.

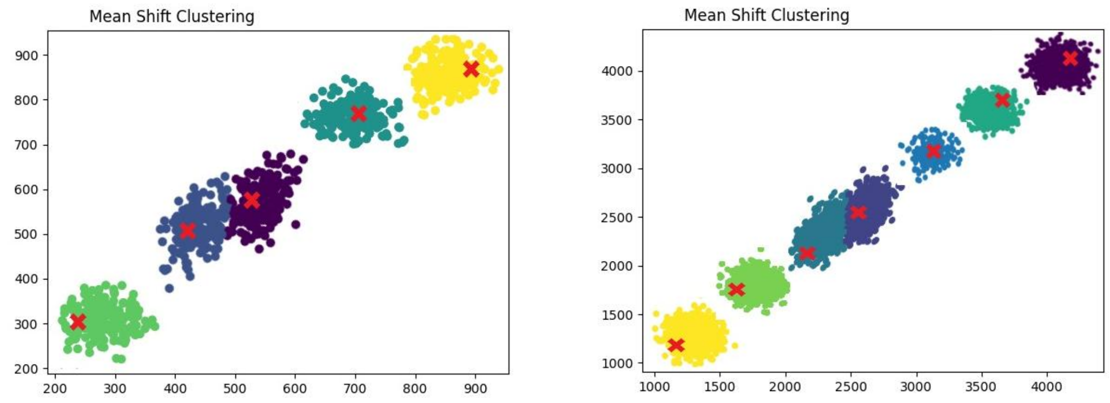

Fig.3. Clusters formed for 1000 stakers (in left image) and 5000 stakers (in right image)

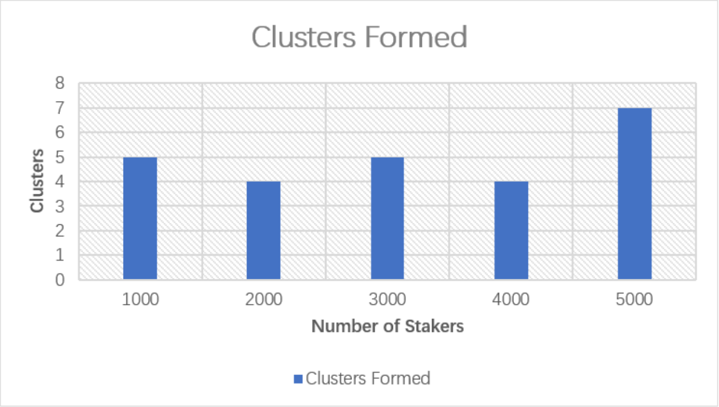

Fig.4. Clusters formed for different stakers

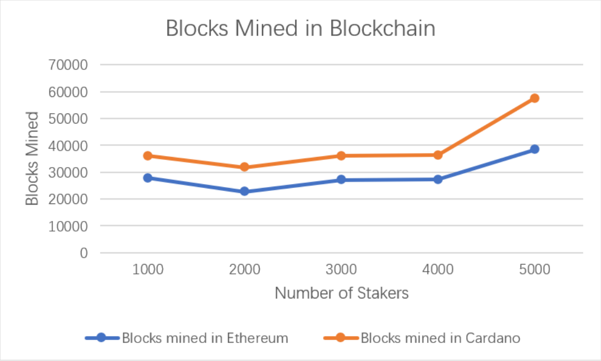

Fig.5. Blocks mined in ethereum and cardano

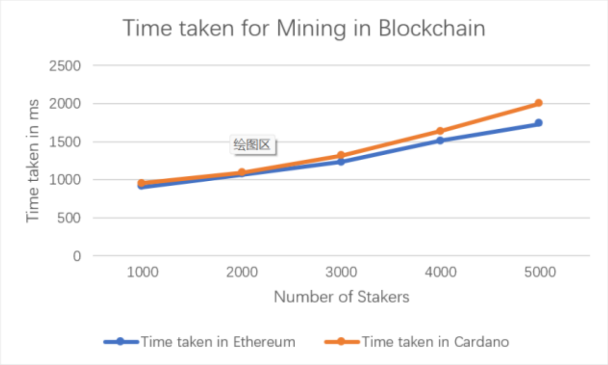

Fig.6. Time taken(ms) for mining in ethereum and cardano

Table 6. Number of clusters formed, cluster members, average and median clusters for different stakers

Number of Stakers	Clusters Formed	Number of Cluster members in each clusters	Average Cluster Size	Median Cluster Size
1000	5	{182, 182, 167, 167, 302}	200	182
2000	4	{464, 354, 441, 741}	500	453
3000	5	{618, 644, 643, 322, 773}	600	643
4000	4	{926, 709, 872, 1493}	1000	899
50000	7	{1027, 534, 534, 534, 534, 534, 1303}	714	534

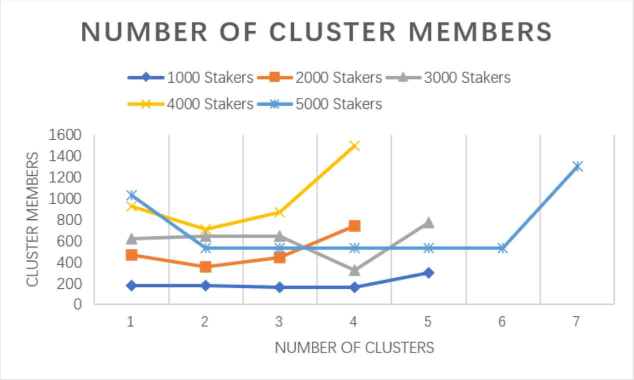

Fig.7. Number of clusters and cluster members

In summary, the suggested SPoS produces better throughput (Scalability) than PoW and PoS. Table 2 shows that it is highly energy-efficient, resistant to attack like 51%, and effective in terms of TPS. In simple terms, SPoS performs better than PoW in every aspect. In addition to having higher TPS than PoS, SPoS is far more resilient than PoS against attacks such as Nothing-at-Stake and coin age accumulation attacks. Consequently, we propose that SPoS fits well with the current blockchain architecture.

Being a desktop application built on Java, JMeter works with a wide range of operating systems and may be used on Windows, Linux, and Mac computers. Because of the JMeter framework's support for concurrent execution, running multiple Threads and Thread Groups is made possible by design. Since JMeter is open source, it can be expanded and supports a large variety of plugins. JMeter is a member of the Apache Software Foundation and is completely free and open source. Its user interface is implemented using the Swing Java API. JMeter is used to assess the suggested system for 5000 clients.

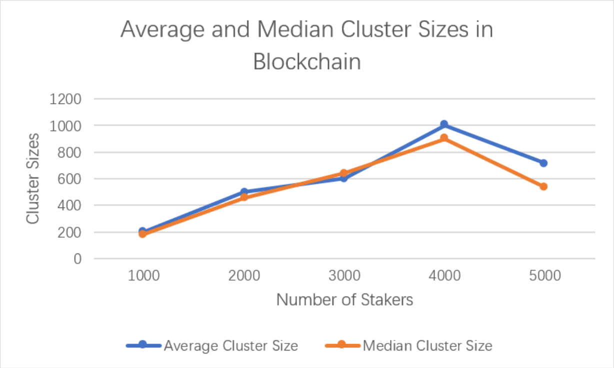

Fig.8. Average and median cluster sizes

5. Conclusions

Application development for PoW-based blockchains is becoming unfeasible due to high computational demands and energy footprint. On other hand, network centralization and unfairness are problems with the widely accepted Proof-of-Stake (PoS) system. We have presented an enhanced Proof of Stake, SPoS, in this paper that resists centralization and brings justice to the blockchain network. This work examines the features and issues with current consensus protocols, such as PoW and PoS, and suggests a new protocol, SPoS, which builds upon PoS. The key innovation is that the SPoS protocol lowers the possibility of a coin age accumulation attack in the system by using quantity of coins rather than their age. We first compared the ways that PoW, PoS, and SPoS differ from each other before simulating SPoS for up to 5000 participants in the blockchain network using Ethereum and Cardano. According to experimental findings, the suggested PoS protocol is more scalable and leads to higher throughput than PoW. It also uses less energy and is resistant to 51% attacks. Put differently, in every aspect, SPoS performs better than PoW. In addition to having higher TPS than PoS, SPoS is far more resilient than PoS against attacks such as Nothing-at-Stake and coin age accumulation attacks. Fair mining is ensured for all stakeholders based on number of stakes. Mining is distributed among all stakeholders. We therefore propose that SPoS is appropriate for the blockchain system in use today. It is impossible to say how many nodes at most can guarantee resilience and stability of SPoS system. In future studies, number of nodes in the SPoS system can be used as variable and simulation-based optimization approaches can be used to determine greatest value. Proposed SPoS consensus algorithm can be used in various real blockchain platforms depending on the applications to achieve scalability, fairness and decentralization.

References

[1] S. Zhang and J. H. Lee, “Analysis of the main consensus protocols of blockchain,” *ICT Express*, vol. 6, no. 2, pp. 93–97, 2020, doi: 10.1016/j.icte.2019.08.001.

[2] B. S. Anupama and N. R. Sunitha, “Analysis of the Consensus Protocols used in Blockchain Networks - An overview,” *IEEE Int. Conf. Data Sci. Inf. Syst. ICDSIS 2022*, pp. 1–6, 2022, doi: 10.1109/ICDSIS55133.2022.9915929.

[3] L. Qi, J. Tian, M. Chai, and H. Cai, “LightPoW: A trust based time-constrained PoW for blockchain in internet of things,” *Comput. Networks*, vol. 220, no. April 2022, p. 109480, 2023, doi: 10.1016/j.comnet.2022.109480.

[4] B. Cao *et al.*, “Performance analysis and comparison of PoW, PoS and DAG based blockchains,” *Digit. Commun. Networks*, vol. 6, no. 4, pp. 480–485, 2020, doi: 10.1016/j.dcan.2019.12.001.

[5] Y. Wang *et al.*, “Study of Blockchains’s Consensus Mechanism Based on Credit,” *IEEE Access*, vol. 7, pp. 10224–10231, 2019, doi: 10.1109/ACCESS.2019.2891065.

[6] A. K. Yadav, K. Singh, A. H. Amin, L. Almutairi, T. R. Alsenani, and A. Ahmadian, “A comparative study on consensus mechanism with security threats and future scopes: Blockchain,” *Comput. Commun.*, vol. 201, no. October 2022, pp. 102–115, 2023, doi: 10.1016/j.comcom.2023.01.018.

[7] H. Xiong, M. Chen, C. Wu, Y. Zhao, and W. Yi, “Research on Progress of Blockchain Consensus Algorithm: A Review on Recent Progress of Blockchain Consensus Algorithms,” *Futur. Internet*, vol. 14, no. 2, 2022, doi: 10.3390/fi14020047.

[8] V. Bachani and A. Bhattacharjya, “Preferential Delegated Proof of Stake (PDPoS)—Modified DPoS with Two Layers towards Scalability and Higher TPS,” *Symmetry (Basel).*, vol. 15, no. 1, 2023, doi: 10.3390/sym15010004.

[9] R. Chen, L. Wang, and R. Zhu, “Improvement of Delegated Proof of Stake Consensus Mechanism Based on Vague Set and Node Impact Factor,” *Entropy*, vol. 24, no. 8, 2022, doi: 10.3390/e24081013.

[10] “DOGECOIN web page,” *Available online : https://dogecoin.com/.*

[11] “Litecoin Web Page,” *Available online : https://litecoin.org/.*

[12] L. Bahri and S. Girdzijauskas, "When Trust Saves Energy: A Reference Framework for Proof of Trust (PoT) Blockchains," *Web Conf. 2018 - Companion World Wide Web Conf. WWW 2018*, pp. 1165–1169, 2018, doi: 10.1145/3184558.3191553.

[13] K. J. O'Dwyert and D. Malone, "Bitcoin mining and its energy footprint," *IET Conf. Publ.*, vol. 2014, no. CP639, pp. 280–285, 2014, doi: 10.1049/cp.2014.0699.

[14] P. Giungato, R. Rana, A. Tarabella, and C. Tricase, "Current trends in sustainability of bitcoins and related blockchain technology," *Sustain.*, vol. 9, no. 12, 2017, doi: 10.3390/su9122214.

[15] E. Symitsi and K. J. Chalvatzis, "Return, volatility and shock spillovers of Bitcoin with energy and technology companies," *Econ. Lett.*, vol. 170, pp. 127–130, 2018, doi: 10.1016/j.econlet.2018.06.012.

[16] H. Vranken, "Sustainability of bitcoin and blockchains," *Curr. Opin. Environ. Sustain.*, vol. 28, pp. 1–9, 2017, doi: 10.1016/j.cosust.2017.04.011.

[17] J. Spasovski and P. Eklund, "Proof of stake blockchain: Performance and scalability for groupware communications," *9th Int. Conf. Manag. Digit. Ecosyst. MEDES 2017*, vol. 2017-Janua, pp. 251–258, 2017, doi: 10.1145/3167020.3167058.

[18] M. Bartoletti, S. Lande, and A. S. Podda, "A proof-of-stake protocol for consensus on bitcoin subchains," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10323 LNCS, pp. 568–584, 2017, doi: 10.1007/978-3-319-70278-0_36.

[19] L. Fan and H.-S. Zhou, "A Scalable Proof-of-Stake Blockchain in the Open Setting ∗ (or, How to Mimic Nakamoto's Design via Proof-of-Stake)," *Cryptol. ePrint Arch.*, 2018, [Online]. Available: https://eprint.iacr.org/2017/656.pdf

[20] A. M. Bentov Iddo, Ariel Gabizon, "Cryptocurrencies Without Proof of Work," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8438, pp. 142–157, 2016, doi: 10.1007/978-3-662-44774-1.

[21] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, pp. 557–564, 2017, doi: 10.1109/BigDataCongress.2017.85.

[22] D. B. and O. R. Kiayias, Aggelos, Russell Alexander, *Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol*, vol. 10403, no. 639554. 2017. doi: 10.1007/978-3-319-63688-7.

[23] J. Garay, A. Kiayias, and Nikos Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications," vol. 9057, pp. 817–836, 2015, doi: 10.1007/978-3-662-46803-6.

[24] R. P. and E. S. Phil Daian, "Snow white: Robustly reconfigurable consensus and applications to provably secure proof of stake," in *International Conference on Financial Cryptography and Data Security*, 2019, pp. 23–41. doi: https://doi.org/10.1007/978-3-030-32101-7_2.

[25] R. Pass and E. Shi, "FruitChains: A fair blockchain," *Proc. Annu. ACM Symp. Princ. Distrib. Comput.*, vol. Part F1293, pp. 315–324, 2017, doi: 10.1145/3087801.3087809.

[26] J. Chen and S. Micali, "Algorand: A secure and efficient distributed ledger," *Theor. Comput. Sci.*, vol. 777, pp. 155–183, 2019, doi: 10.1016/j.tcs.2019.02.001.

[27] B. Wang, Z. Li, and H. Li, "Hybrid consensus algorithm based on modified proof-of-probability and DPoS," *Futur. Internet*, vol. 12, no. 8, pp. 1–16, 2020, doi: 10.3390/FI12080122.

[28] MoonKing, "Supernode Proof of Stake Consensus Complete Guide by MoonKing9998," 2019. https://medium.com/@moonking9998/supernode-proof-of-stake-complete-guide-by-moonking9998-41a8f7675a28

[29] C. Badertscher, P. Gaži, A. Kiayias, A. Russell, and V. Zikas, "Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability," *Proc. ACM Conf. Comput. Commun. Secur.*, no. 780477, pp. 913–930, 2018, doi: 10.1145/3243734.3243848.

[30] S. King and S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," *Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS'16*, vol. 1919, no. January, pp. 1–27, 2017, [Online]. Available: http://peerco.in/assets/paper/peercoin-paper.pdf%0Ahttp://fc17.ifca.ai/preproceedings/paper_73.pdf%0Ahttp://arxiv.org/abs/1606.06530%0Ahttps://papers.ssrn.com/sol3/papers.cfm?abstract_id=2977811%0Ahttp://dl.acm.org/citation.cfm?doid=2976749.2978389%0Ahttp

[31] G. Fanti, L. Kogan, S. Oh, K. Ruan, P. Viswanath, and G. Wang, "Compounding of Wealth in Proof-of-Stake Cryptocurrencies," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11598 LNCS, pp. 42–61, 2019, doi: 10.1007/978-3-030-32101-7_3.

[32] M. Li *et al.*, "CrowdBC: A blockchain-based decentralized framework for crowdsourcing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 6, pp. 1251–1266, 2019, doi: 10.1109/TPDS.2018.2881735.

[33] V. Buterin, "Proof of Work is the Rich Get Richer Squared" Says Vitalik Buterin," 2018. https://www.trustnodes.com/2018/07/10/proof-work-rich-get-richer-squared-says-vitalik-buterin

[34] M. Saad, V. Cook, L. Nguyen, M. T. Thai, and A. Mohaisen, "Partitioning attacks on bitcoin: Colliding space, time, and logic," *Proc. - Int. Conf. Distrib. Comput. Syst.*, vol. 2019-July, pp. 1175–1187, 2019, doi: 10.1109/ICDCS.2019.00119.

[35] M. Saad *et al.*, "Exploring the Attack Surface of Blockchain: A Comprehensive Survey," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1977–2008, 2020, doi: 10.1109/COMST.2020.2975999.

[36] T. Duong, A. Chepurnoy, L. Fan, and H.-S. Zhou, "TwinsCoin: A Cryptocurrency via Proof-of-Work and Proof-of-Stake," pp. 1–13, 2018, doi: 10.1145/3205230.3205233.

[37] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake," *Cryptol. ePrint Arch.*, vol. 452, no. 3, pp. 1–19, 2014.

[38] W. Li, S. Andreina, J. M. Bohli, and G. Karame, "Securing Proof-of-Stake Blockchain Protocols Wenting," *Proceedings*, pp. 297–315, 2017, doi: 10.1007/978-3-319-67816-0.

[39] F. Saleh, "Blockchain Without Waste: Proof-of-Stake," *SSRN Electron. J.*, no. May, 2018, doi: 10.2139/ssrn.3183935.

[40] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," *2018 41st Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2018 - Proc.*, pp. 1545–1550, 2018, doi: 10.23919/MIPRO.2018.8400278.

[41] X. Wei, A. Li, and Z. He, "Impacts of consensus protocols and trade network topologies on blockchain system performance," *Jasss*, vol. 23, no. 3, pp. 1–20, 2020, doi: 10.18564/jasss.4289.

[42] Z. Hussein, M. A. Salama, and S. A. El-Rahman, "Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms," *Cybersecurity*, vol. 6, no. 1, 2023, doi: 10.1186/s42400-023-00163-y.

[43] M. I. Mehar *et al.*, “Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack,” *J. Cases Inf. Technol.*, vol. 21, no. 1, pp. 19–32, 2019, doi: 10.4018/JCIT.2019010102.

[44] L. Mearian, “MIT’s blockchain-based ‘Spider’ offers 4X faster cryptocurrency processing,” *2020*. https://www.computerworld.com/article/3518893/mits-blockchain-based-spider-offers-4x-faster-cryptocurrency-processing.html

Authors’ Profiles

Anupama B. S. is currently pursuing her Ph.D. in Computer Science and Engineering from Visvesvaraya Technological University, Belagavi, India. She earned her M.Tech. in Computer Networks Engineering and B.E. in Computer Science and Engineering from Visvesvaraya Technological University (VTU), Belagavi, India in the years 2013 and 2011 respectively. She has published papers in various reputed International Conferences. Her research interests include Blockchain Technology, Machine Learning, Cryptography, IOT and Deep Learning.

Dr. N. R. SUNITHA received B.E. degree from Gulbarga University, M.S. degree from Birla Institute of Technology and Science, and Ph.D. degree from Visveswaraya Technological University, Belgaum. She is currently Professor with Department of CS&E, Siddaganga Institute of Technology, India. She has published more than 65 peer-reviewed research articles in leading conferences and journals, such as ACM, Springer, the IEEE, and Elsevier. Her research interests include cryptography and network security, storage area networks, big data processing, industrial automation, and computer security and reliability. She was funded for her research projects from ABB GISL, AICTE, DRDO, IISc, and ICT Skill Development Society in India. She has acquired totally six patents in her research field. Dr. Sunitha possesses membership of personal bodies in Association of Computing Machinery, USA (ACM), Indian Society for Technical Education, India (ISTE)—Life Member, Computer Society of India (CSI), International Association of Engineers (IAENG), and Institution of Engineers (FIE). She received IBM Mentor Award, in 2014. She was a chairperson in international conferences, such as Conference on Information Science and Technology Management (CISTM 2007), Conference on Network Security and Applications (CSNA 2010), National Conference on Advances in Computer Applications (NCACA), and International Conference on Advances in Computing (ICAdC 2012). Her biodata included in Marquis Who’s Who in Science & Engineering 2010. She is a Reviewer of journals, such as Elsevier’s Computers and Security and International Journal of Network Security (IJNS)

Dr. G. S. Thejas is Assistant Professor at Department of Computer Science and Electrical Engineering at Tarleton State University (TSU), Texas A&M University System, since 2020. His research areas include Machine Learning, Deep Learning, Click Fraud Detection, Cybersecurity, Human-Computer Interaction (HCI), and Performance Optimization using Parallel Computing. He directs Machine Intelligence and Security Research Laboratory (MISR Lab). He worked as trainee for one year at Defence Research and Development Organization/Electronic and RADAR Development Establishment (DRDO/LRDE). He worked as Assistant Professor for five years at Siddaganga Institute of Technology (SIT), India. He is recipient of Best Graduate Student in Service Award, Dissertation Year Fellowship Award, two times FIU School of Computing and Information Sciences travel Award, FIU Graduate and Professional Student Committee (GPSC) travel grant, and Graduate Assistantship award at FIU. Thejas's research has successfully produced several papers in top conferences and journals like ACM, IEEE, Springer, Elsevier, and MDPI. He is member of Institute of Electrical and Electronics Engineers (IEEE) and Association for Computing Machinery (ACM). Elsevier News Board: Based on work entitled "A hybrid and effective learning approach for Click Fraud detection" has been recognized and appeared in Elsevier's news board as "Curbing the clicking con: The automated detection of click fraud", May 25, 2021.

How to cite this paper: Anupama B. S., Sunitha N. R., G. S. Thejas, "Scalable-pos: Towards Decentralized and Efficient Energy Saving Consensus in Blockchain", International Journal of Computer Network and Information Security(IJCNIS), Vol.17, No.6, pp.84-97, 2025. DOI:10.5815/ijcnis.2025.06.06