Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.055908

ARTICLE

Leveraging Sharding-Based Hybrid Consensus for Blockchain

Hind Baageel[1] and Md Mahfuzur Rahman[1,2,*]

[1]Department of Information & Computer Science, King Fahd University of Petroleum & Minerals, Dhahran, 31261, Saudi Arabia

[2]Interdisciplinary Research Center (IRC) for Intelligent Secure Systems, King Fahd University of Petroleum & Minerals, Dhahran, 31261, Saudi Arabia

*Corresponding Author: Md Mahfuzur Rahman. Email: mdmahfuzur.rahman@kfupm.edu.sa

Received: 10 July 2024 Accepted: 11 September 2024 Published: 15 October 2024

ABSTRACT

The advent of blockchain technology has transformed traditional methods of information exchange, shifting reliance from centralized data centers to decentralized frameworks. While blockchain's decentralization and security are strengths, traditional consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS) face limitations in scalability. PoW achieves decentralization and security but struggles with scalability as transaction volumes grow, while PoS enhances scalability, but risks centralization due to monopolization by high-stake participants. Sharding, a recent advancement in blockchain technology, addresses scalability by partitioning the network into shards that process transactions independently, thereby improving throughput and reducing latency. However, cross-shard communication, essential for transactions involving multiple shards, introduces challenges in coordination and fault tolerance. This research introduces a shard-based hybrid consensus model, PoSW, which combines PoW and PoS to mitigate the limitations of both mechanisms. By integrating PoW's fairness with PoS's scalability in a shard-based blockchain, the proposed model addresses key issues of scalability and monopolization. We evaluate the model against state-of-the-art consensus algorithms, including Monoxide and Practical Byzantine Fault Tolerance (PBFT). The results show that the proposed PoSW model reduces communication overhead compared to PBFT and improves resource utilization over Monoxide. In addition to performance gains, the security analysis demonstrates that the PoSW model provides robust defense against common blockchain attacks such as the 51% and Sybil attacks, etc. The proposed approach is particularly suited for applications like decentralized finance (DeFi) and supply chain management, which require both high scalability and robust security. The contributions of this research include the development of the PoSW hybrid consensus mechanism, its comparative evaluation with leading algorithms, and a thorough security analysis. These contributions represent a significant step forward in addressing blockchain's scalability, fairness, and security challenges.

KEYWORDS

Blockchain; consensus algorithm; decentralized network

1 Introduction

Blockchain technology was initially used for digital currency, but it has since expanded to a wide range of applications, including healthcare, education systems, network management, and various

other fields that utilize blockchain as a secure ledger for their data. The emergence of blockchain technology in the internet era has revolutionized conventional methods of information exchange, ushering in a paradigm shift away from reliance on centralized data center practices. Offering a decentralized framework, blockchain comprises immutable blocks of transactions. Furthermore, it employs miners capable of verifying and validating transactions based on predetermined conditions prior to their inclusion in the blockchain ledger. For blockchain miners to agree on the network's state and transaction validity, the blockchain follows a consensus protocol. This protocol ensures the integrity and security of the blockchain by preventing double-spending and maintaining a consistent, tamper-proof record of all transactions. However, it is widely acknowledged as the blockchain trilemma, positing that only two out of the following three properties can be simultaneously met: scalability, security, and decentralization [1]. Nevertheless, the expansion of blockchain networks has presented challenges concerning infrastructure scalability, size, and usage. Despite their efficacy in ensuring decentralization, traditional consensus mechanisms such as Proof of Work (PoW) and proof of stake (PoS) struggle to maintain high throughput in large-scale networks. In Proof of Work (PoW) consensus mechanism, decentralization, and security are achieved, yet scalability falters when confronted with a high volume of users and transactions. Similarly, in the Proof of Stake (PoS) protocol, scalability, and security are attained, but decentralization suffers due to the issue of monopolization, wherein miners with substantial stakes dominate the network, leaving those with lower stakes with limited opportunities for participation.

One of the recent advancements in blockchain technology aimed at addressing scalability issues is the adoption of sharding-based blockchain. Unlike traditional blockchain systems where every transaction requires verification by all miners or nodes, sharding permits subsets of transactions to be delegated to groups of nodes. In this paradigm, nodes collaborate within their respective groups to achieve consensus and process transactions. The parallel processing of transactions results in a significant boost in scalability. Sharding can be categorized into two types: cross-shard and non-cross-shard. Cross-shard sharding involves communication and coordination between different shards for transactions spanning multiple shards, while non-cross-shard sharding confines transactions to individual shards, reducing complexity but potentially limiting inter-shard interaction. Sharding the blockchain offers several advantages, including increased throughput. In a shard-based blockchain, throughput is enhanced because each shard processes its transactions independently of others, allowing for parallel transaction processing at the shard level [2]. Additionally, sharding reduces latency since each shard handles a smaller number of transactions, which decreases the time required for validation and verification processes. Moreover, Sharding enhances the overall security of the blockchain system by reducing the attack surface. However, Yu et al. [3] have conducted a security analysis demonstrating that cross-shard communication can offer more security compared to non-cross-shard communications. Nevertheless, cross-shard communication introduces the challenge of ensuring smooth interactions between shards for transactions that span multiple shards. Additionally, a robust fault tolerance policy is crucial to manage the failure of individual shards and ensure the system's overall availability. Effective management of sharding includes coordinating cross-shard communications, balancing workloads, and ensuring robust fault tolerance to maintain overall network efficiency and security.

In this research, we introduce a shard-based hybrid consensus approach–"PoSW" that integrates Proof of Work (PoW) and Proof of Stake (PoS) to mitigate their inherent limitations. Our shard-based approach plays a pivotal role in the proposed model, offering effective solutions for issues related to fairness and scalability. Specifically, we aim to address the scalability challenges of PoW and the monopolization tendencies of PoS by integrating them into a sharding-based blockchain architecture.

The proposed model has been simulated and evaluated based on performance and security metrics. We compared it to state-of-the-art consensus methods, such as the Monoxide [4] and Practical Byzantine Fault Tolerance (PBFT) [5] algorithms. Experimental results demonstrate that our model provides better resource utilization compared to the Monoxide algorithm and reduces communication overhead compared to PBFT, primarily through the strategic use of PoW. In summary, our shard-based hybrid consensus approach not only addresses the limitations of PoW and PoS but also enhances the overall efficiency and security of blockchain systems. The proposed Sharding-based Hybrid Consensus model is particularly well-suited for applications that require both high scalability and robust security. This model is ideal for decentralized finance (DeFi) platforms, where rapid transaction processing and security against attacks are critical. Additionally, it fits well with supply chain management systems, where multiple parties need to collaboratively validate transactions efficiently across different segments of the supply chain. The hybrid approach of PoS and PoW ensures that the network remains secure while scaling to accommodate a high volume of transactions, making it advantageous for applications that demand both performance and resilience in a distributed environment. The contributions of this research can be summarized as:

i) Introduction of Shard-based Hybrid Consensus Approach (PoSW) which combines Proof of Work (PoW) and Proof of Stake (PoS) to mitigate their inherent limitations that effectively address issues related to scalability and fairness.

ii) Comparison between the proposed model and State-of-the-Art Consensus Methods such as Monoxide and Practical Byzantine Fault Tolerance (PBFT) algorithms. The proposed model proved to reduce communication overhead compared to PBFT, mainly through the strategic use of PoW, and demonstrates better resource utilization than Monoxide.

iii) The security analysis of the proposed model against popular blockchain attacks such as the 51% attack and Sybil attack. Experimental results demonstrate that the shard-based hybrid consensus (PoSW) approach provides a strong defense against such attacks.

The rest of the paper is organized as follows. Section 2 provides an overview of the existing techniques through a literature review. Section 3 delves into the proposed methodology with system architecture. Section 4 presents the experiment setups, results and facilitates discussion, while the paper concludes with some future work in Section 5.

2 Related Work

The exploration of sharding-based solutions within blockchain technology has been extensive, driven by the need to overcome the inherent limitations of traditional consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS). Researchers have extensively analyzed the blockchain trilemma, which posits that achieving scalability, security, and decentralization simultaneously is a significant challenge. Various approaches have been proposed to address this trilemma, including sharding, hybrid consensus models, and enhancements to existing protocols. In this section, we review the state-of-the-art in shardingbased blockchain solutions, highlighting their methodologies, strengths, and limitations.

Song et al. [6] introduced a new consensus method called proof of contribution (PoC), which relies on assigning contribution values to miners to validate new blocks for intellectual property protection. The node with the highest contribution value is designated to generate the new block in the blockchain. The authors also addressed the defense against consecutive fake transactions attempting to gain contribution nodes. To counter spam attacks, they proposed a cooling function

that reduces the accrued contribution value when consecutive block registrations occur within a short timeframe. However, if an attacker persists in targeting the blockchain at various time intervals, there is a potential risk of compromising its integrity. Moreover, there is a risk of centralization for nodes with exceptionally high contribution values. Such nodes have the potential to dominate the creation of new blocks, and this dominance may be exploited to introduce fake transactions into the blockchain. Another consensus method proposed by Manolache et al. [7] is known as Proof of Authority (PoA). In this consensus approach, miners are identified based on real and accurate data about their identity. Similar to Proof of Contribution (PoC), this method shares the advantage of offering faster transaction times and requiring fewer computational resources compared to Proof of Work (PoW). However, it has limitations, notably its lack of full decentralization because it relies on identity validators. Another comparable consensus approach is proposed by Rosli et al. [8], known as Proof of Trust (PoT). In this method, data authentication involves a trust anchor facilitated by a validation group and a leader. The leader is selected based on receiving the highest votes from half of the nodes.

The preeminence of the Proof of Work (PoW) consensus mechanism is widely acknowledged in the blockchain domain, yet it has drawbacks. One notable challenge is the potential for reduced throughput when the difficulty level becomes excessively high for selected miners. In Reference [7], an alternative approach is proposed by the authors, introducing an augmented version of PoW that leverages Reinforcement Learning (RL) techniques. In this model, RL is employed to dynamically learn and adjust the optimal difficulty level, aiming to mitigate issues related to fairness and minimize mining time. It is important to note, however, that implementing this model necessitates substantial resources for training the RL component within a specific application environment. Masseport et al. [9] proposed another enhancement to PoW by giving a fair chance to minors with limited computation resources. This fairness is delivered by giving these minors lower difficulty levels according to their contribution to the blockchain if they don't reach a solution.

In Reference [9], the authors proposed a hybrid approach that combines both Proof of Work (PoW) and Proof of Stake (PoS) consensus methods. These methods address concerns such as low throughput, unfair miner selection, susceptibility to 51% attacks, and double-spending risks. Our proposed model addresses these issues by integrating these consensus methods into a shard-based blockchain. This model introduces parallelism through sharding, enabling the simultaneous processing of multiple transactions to tackle the problem of low throughput. Furthermore, by assigning different shards and nonce difficulty levels based on stakes, the model ensures a fair opportunity for nodes with lower stakes to participate in the blockchain. In Reference [4], the authors proposed a sharding-based model that uses PoW as the consensus method within each shard, addressing scalability issues inherent in PoW. Miners are randomly assigned to each shard, where they solve puzzles and mine the required blocks. Our proposed model shares a similar sharding architecture but differs in the miner assignment method. Instead of random assignment, miners in our model are assigned to shards based on PoS. Unlike the equal treatment of shards in Monoxide, our proposed PoSW introduces a hierarchical structure, dividing shards into different levels. This hierarchy improves resource utilization and fosters more coherent groups of miners.

We also compare our proposed hybrid consensus approach with these existing methods to illustrate its unique contributions and advantages (Refer to Table 1). In comparison to previous work, our proposed shard-based hybrid consensus model, which integrates PoW and PoS, addresses the scalability and fairness challenges more effectively by introducing hierarchical shard levels and a PoS-based miner assignment method. This approach ensures better resource utilization and creates more coherent miner groups, enhancing both the security and efficiency of the blockchain system. Additionally, the proposed model focuses on reducing the risk of centralization by implementing

a randomized shuffling mechanism for shard assignments, thereby promoting a more distributed and equitable network. Additionally, while a prominent scheme like OmniLedger [22] may encounter scalability issues due to its epoch-based notarization process, our model employs hierarchical shard levels and a shard-based hybrid consensus approach. This design facilitates parallel transaction processing, resulting in significantly enhanced scalability and throughput.

Table 1: Comparison between different consensus methods

Ref.	Model	Strengths	Limitations
[6]	Proof of Contribution: Consensus method based on contribution value to add new blocks to the blockchain	Incentives extend beyond digital currency and encompass non-monetary rewards like reputations and contribution values. Reduced environmental impact	Decentralization risk for nodes with high contribution values. Attackers may exploit the system by executing fake transactions to acquire contribution value persistently at different time intervals.
[7]	Proof of Authority: Consensus method that required real and accurate data on miners' identities to validate them for adding new blocks	Higher transaction rate than PoW, Predictable block generation time, Strong security because of node authentication mechanism	Not fully decentralized because of the reliance on identity validators. The identity of validators must be known to everyone which might make them an attack target.
[8]	Consensus through "Proof of Trust" involves a voting process using the Raft algorithm to select a leader. The chosen leader takes on the responsibility of forming a validating group tasked with authenticating data, utilizing a trust anchor	Higher transaction rate than PoW, Efficient resources requirements	Nodes are required to submit the commands to a voted leader which is a centralized entity and that violates to concept of decentralization.

(Continued)

Table 1 (continued)

Ref.	Model	Strengths	Limitations
[5]	Sharding-based blockchain with consensus using Practical Byzantine Fault Tolerance (PBFT)	This approach tackles the scalability issue in blockchain applications by breaking down transactions into smaller parts called shards. It enables various nodes (members of these shards) to collaborate in addressing the associated challenges	Security concern: if a shard contains more malicious actors than honest actors, the malicious actor can gain control over the block generation and manipulate transactions validation through multiple shards requires constant and accurate communication which leads to increased latency and overhead.
[9]	Proof of Experience: Improved Proof of Work with previous minor experience	This scheme gives fair opportunity to minors with limited computational resources	The model was not evaluated mathematically or experimentally.
[10]	Two-tiered consensus mechanism based on PoW and PoS	The proposed model addresses problems of 51% attack, double spending problem, and unfair minor selection	Scalability issues due to PoW.
[11]	Proof of Majority: Considering 90% of votes as true transaction	The proposed method proved to provide faster transaction time without requiring extensive computational results	Significant workload when nodes are greater than 20. Vulnerability to Sybil attacks where large amounts of fake identities are used to control the network.
[4]	Monoxide: Scale Out Blockchain with Asynchronous Consensus Zones where each zone operates independently	No intra-class communication is required between zones which leads to reduced communication overhead	Random assignment of miners to zones can result in inefficient resource allocation.
[12]	Proof of Burn (PoB): Miners are required to destroy (Burn) their cryptocurrency as proof of their investment	Low energy consumption and high security	Participants risk losing the value of the burned tokens if the network does not succeed. There is a risk of centralization, as miners with a large number of tokens can dominate the network [13].

(Continued)

Table 1 (continued)

Ref.	Model	Strengths	Limitations
[14]	Delayed Proof of Work (dPoW): This scheme uses a secondary blockchain to protect the main blockchain	High security and reliability	Increased complexity and difficulty of implementation compared to traditional PoW. dPoW has compatibility issues, as it may not work on certain types of hardware [13].
[15]	Scalable blockchain protocol based on proof of stake and sharding	High scalability and security	The proposed model does not address the monetization issue associated with the PoS consensus method.
[16]	Location-based Sharding in Fog Computing Networks	Reduce consensus latency and improve throughput	Shards can become concentrated in specific locations, leading to uneven resource allocation, increased susceptibility to localized attacks or network failures.
[17]	A blockchain dynamic sharding scheme based on the Hidden Markov Model in IoT	Enhance modularity, transaction throughput, and confirmation latency	The complexity of accurately predicting and adapting to dynamic changes in the IoT environment can result in computational overhead and uneven shard reallocation.
[18]	Sharding based on priority scheme	Improve processing time for prioritized processes and reduce network congestion	Lower-priority transactions can suffer from starvation and experience significant delays.
[19]	Secure Sharding Scheme of Blockchain-based on Reputation and Verifiable Random Functions (VRF)	Enhances security and the proposed scheme motivates honest nodes to remain active, increases overall throughput	Attacks on reputation scores can lead to undue influence, compromising the security and fairness of the network.

(Continued)

Table 1 (continued)

Ref.	Model	Strengths	Limitations
[20]	Meepo: Sharded consortium blockchain	Enhances cross-shard efficiency via the cross-epoch and cross-call. Furthermore, the proposed model uses a backup algorithm (shadow shard) based recovery to improve the shard robustness	An increased number of shards can lead to hotspot account problems, which in turn reduces throughput [21].
[22]	OmniLedger: Decentralized ledger via sharding	Scale-out effectively while maintaining overall system security, concurrent (parallel) transaction execution	OmniLedger is not well-suited for dealing with adaptive adversaries because it takes a long time to set up each epoch. This delay in updating the ledger can allow malicious actors to exploit the system before the next epoch begins [21].

3 Methodology

3.1 System Model

This research aims to develop a hybrid consensus approach for blockchain tailored for safeguarding monopolization and increased overall security. The envisioned model starts with a mempool of transactions awaiting to be processed by miners for subsequent integration into the blockchain. The hybrid consensus mechanism is activated by initially assigning mining nodes to network shards using Proof of Stake (PoS). For instance, miners with stakes higher than a certain shard threshold will be assigned to that shard until it becomes full. Next, transactions of mempool are assigned to network shards proportionately so that all the shards receive sufficient mining tasks. Then, the rest of the work will be done internally within the shard as follows:

Step 1: Within the shard, miners engage in competitive endeavors enhancing their stake and collection of block rewards.

Step 2: Miners are assigned to shards based on their stake. The proposed blockchain infrastructure is divided into three levels—High, Mid, and Low—to which miners are allocated according to their stake.

Step 3: Multiple Proof of Work (PoW) difficulty levels are used based on the number of shards and number of nodes in a shard.

Step 4: Once miners are assigned to a shard, they can begin mining by discovering a specific nonce that meets the puzzle difficulty requirement. The difficulty of the puzzle, such as the number of leading zeros, is customized based on the computational capacity of the shard. For instance, the "HIGH" shard, populated by miners with superior capabilities, will be assigned a higher PoW difficulty. Miners within this shard are incentivized to tackle the more challenging task because they stand to gain

greater rewards. Conversely, users seeking expedited transaction processing may opt to pay higher fees. Transactions offering higher fees are directed to the "HIGH" shard, where they can be swiftly processed by miners boasting the network's top computational power.

Step 5: Miners who successfully solve the puzzle (by identifying the correct nonce) are rewarded.

Step 6: Miners in all shards are reshuffled internally after a certain period.

The algorithm for efficiently managing miner assignments and validating blocks within the proposed blockchain infrastructure is detailed in Algorithm 1. The algorithm begins by defining the inputs, which are an array of miners with associated values for stake and block rewards (Lines 1–3), and an array of shard levels based on stake, each with a maximum number of miners it can accommodate. The Miner class initializes a miner's stake attribute with a given value (Lines 4–6). The Assign_miner_to_shard function sorts the miners in descending order based on their stake (Lines 7–8), initializes an empty dictionary to hold shard assignments (Line 9), and then iterates over each miner to assign them to a shard (Lines 10–20) based on the given stake. Miners are assigned to the first shard level that has available capacity (Lines 12–16), and any miners who cannot be assigned to a shard are added to a remaining miners list (Lines 17–19). The function returns the shard assignments and the list of remaining miners (Line 20). The Block Validation function checks if a shard solves a puzzle (PoW) (Line 22) and, if successful, adds the corresponding transaction to the blockchain (Line 23).

Algorithm 1: Assigning miners to shards and block validation

```
1 Input: Miners, Shard_levels
2   Miners is an array of miners with associated values (S for stake and R for block rewards)
3   Shard_levels is an array of shards levels based on stake with size attribute (maximum no. of
    miners)
4  Class Miner:
5    Function Initialization (self, stake):
6       self.s = stake   # Initialize the stake attribute
7  Function Assign_miner_to_shard(miners, Shard_levels):
8       sorted_miners = sort_descending (miners, key=s)
9       shard_assignments = {level: [] for level in shard_levels}
10          For miner in miners:
11                    assigned = False
12                    For level, size in shard_levels.items():
13                          IF len(shard_assignments[level]) < size:
14                                shard_assignments[level].append(miner)
15                                assigned = True
16                                break
17                    IF not assigned:
18                    # If all shards are full, add the miner to the remaining miners' list
19                          remaining_miners.append(miner)
20          return shard_assignments, remaining_miners
21  Function Block Validation(Shard, transaction)
22       If (on_solve_puzzle(Shard)):
23                  add_block_to_blockchain(transaction)
```

3.2 Shard-Level Robustness

To ensure the robustness of the proposed model against possible blockchain attacks, the nodes within each shard must be reshuffled periodically to avoid long-range attack. Long-range attack happens when specific miners gain access to the network for an extended period and try to rewrite the history of the blockchain by creating an alternate chain from a point in the past. Reshuffling nodes within a shard after a certain period will prevent nodes from gaining enough influence over the network.

4 Evaluation

4.1 Experimental Setup

The research utilized a simulation tool called BlockSim, created by Alharby et al. [23], to evaluate the proposed model. BlockSim offers simulation capabilities for various blockchain models such as Bitcoin, Ethereum, and other platforms. In the proposed system, miners' work on the block is distributed among shards with the aim of enhancing throughput and offering miners a greater opportunity to engage in the network. The miners in the miners' pool are assigned to the available shard according to its stake (miner stake). In the simulation process, we propose three levels of shards: high, mid, and low level shards. The level of shards is determined by a threshold on the miner's stake. For example, a high level shard accepts miners who have a stake greater than T_h, where T_h is a threshold hyper-parameter specified by the blockchain. Similarly, mid-level shard accepts miners who have stake value between T_m and T_h.

Another hyper-parameters $S_{capacity}$ needs to be specified by the blockchain which specifies the number of miners in each level. In theory, high level shards can accept fewer miners and low level shards should accept a higher number of miners to overcome Bayesian faults. We propose a higher number of miners in Low-Level shards because a greater number of miners have lower chances of failure [24]. Moreover, an increased miner count enhances the likelihood of having honest nodes, thereby augmenting data redundancy. Consequently, it becomes more challenging for an attacker to alter the network's state. Thus, specifying the capacity in each shard level is important to maintain blockchain robustness to byzantine faults or deliberate attacks.

The workflow of the Blocksim tool with the base model is shown in Fig. 1. Blocksim tool is used to test the throughput of the proposed model with different model input parameters like the number of transactions, number of shards, number of miners in a single shard, and others. The input parameters are described in Table 2. We modified the implementation of BlockSim to work with the proposed hybrid consensus method as described in Section 3. In this experiment, we used a laptop with M2 CPU and 16 GB RAM running on MAC OS. To show the capability of the proposed model, we tested it using different input parameters and considered the running time. The results of the experiment are described in the next section.

4.2 Performance Analysis

Initially, we evaluated the performance of our proposed model under two configurations: one without sharding (the base model) and the other utilizing sharding. The summarized results of our simulation are presented in Table 3. The default settings of blocksim were maintained, with a fixed 600-block interval (average time to generate a block) and a 0.5 block propagation delay. It is evident from the findings that the sharding-based approach enhances blockchain throughput by distributing tasks

across multiple shards capable of processing transactions in parallel. On average, the sharding-based blockchain demonstrates a 4% increase in throughput compared to the non-sharding counterpart.

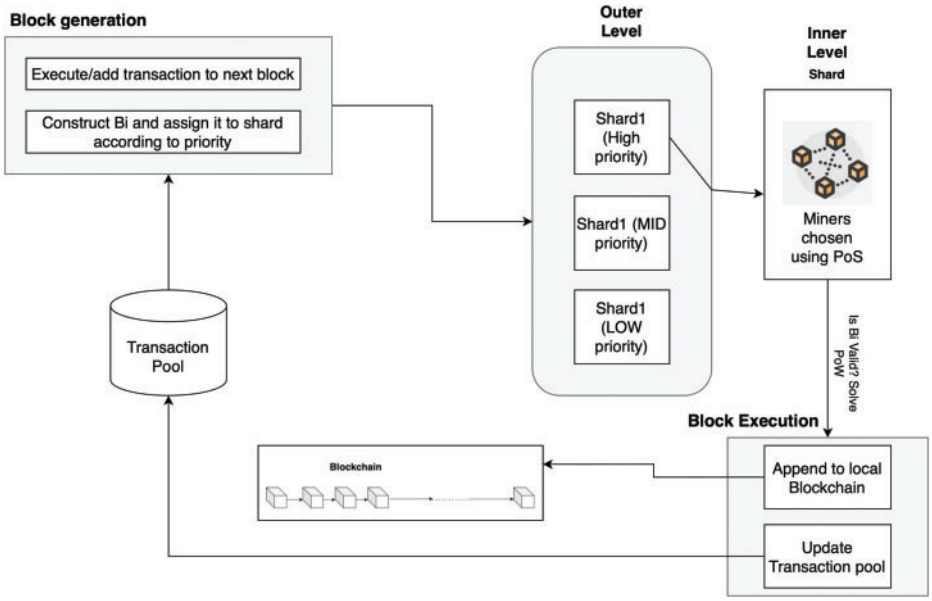

Figure 1: Workflow of the base model implemented in BlockSim simulator

Table 2: Input parameters in BlockSim

Input	Description
$B_{interval}$	Average time to generate a block
B_{Size}	Block size in megabytes (MB)
B_{Delay}	Propagation delay of blocks in seconds
B_{Reward}	Block generation reward
hasTrans	Enable/disabled transactions
T_n	Transactions creation rate
T_{Delay}	Transaction propagation delay of transactions in seconds
T_{fee}	Transaction fees
N_n	Total number of nodes
Sim_{time}	Total simulation time
$Runs$	Number of simulation runs
M_{stake}	Stake value of a miner

During the second testing phase, we examined how the number of miners affects throughput. We varied the number of miners across 5, 10, 20, 30, 50, and 100 in each shard and measured the throughput of the three shard levels accordingly (refer to Table 3 and Fig. 2). The results show that increasing the number of miners leads to a decrease in throughput. The decline in throughput can be attributed to the increased communication overhead associated with a higher number of miners. This

leads to a reduction in the time available to process each transaction. Thus, it is safe to say that around 10 miners in each shard is recom- mended. Less than 10 miners can increase the chance of a 51% attack as discussed later in this section.

Table 3: Simulation results of throughput on sharding-based *vs.* non-sharding blockchain

Number of miners	Throughput (transactions per second)	
	Without sharding	With sharding
5	3.1	8.96
10	2.5	8.8
20	4	7.88
30	2.77	7.7
50	3.3	5.3
100	2.9	4.39

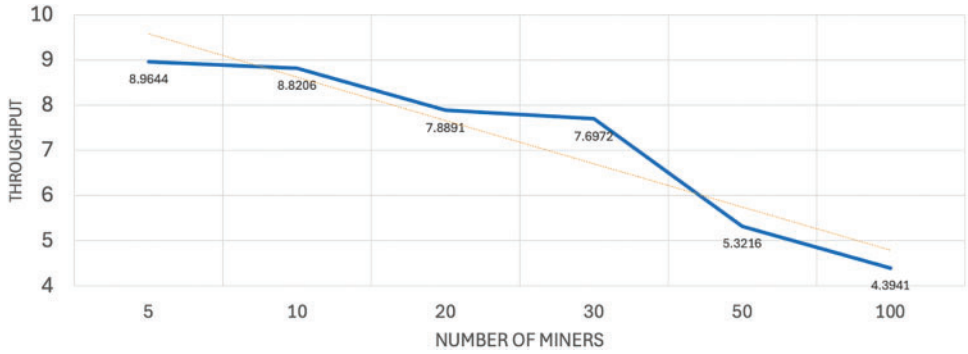

Figure 2: Performance analysis of the proposed model with variations in the number of miners

During the third phase of testing, the block interval served as the target variable, with running time, stale rate, and throughput examined as dependent factors. The stale rate represents the frequency at which a mined block fails to be successfully added to the blockchain due to network delays or other communication issues. As indicated by the data presented in Table 4, a shorter block interval resulted in a substantial increase in running time and a high stale rate of 22%. Conversely, extending the block interval led to reduced running time and a 0% stale rate, although at the cost of decreased throughput at 600 block interval.

Finally, a fairness experiment was conducted using three trials to evaluate the model's bias towards miners with higher hash power. In this experiment, miners were assigned varying levels of mining power to test whether the model favored those with greater computational capacity. The results, displayed in Fig. 3, illustrate the average distribution of blocks mined by different miners. The distribution percentages—ranging from 1.85% to 12.96%—indicate that the proposed model successfully provides a fair chance for miners with varying levels of computational power to participate in the blockchain network. Despite the differences in individual contributions, with some miners holding a higher percentage of the total computational power, all miners, regardless of their capacity, are granted opportunities to contribute to block validation. This variation in distribution demonstrates the model's effectiveness in maintaining fairness, ensuring that even miners with lower computational power are

not excluded from the mining process. Consequently, the model mitigates centralization risks and promotes a more inclusive and balanced network.

Table 4: Simulation results of variations on block interval with fixed simulation time at 30,000 s

Block interval (in seconds)	Actual running time (in seconds)	Stale rate (in %)	Throughput (transactions per second)
1	3.6	22%	17.424
5	0.52	7%	20.52
12	0.52	2%	21.78
60	0.43	0%	22.14
150	0.34	0%	21.75
600	0.43	0%	7.7047

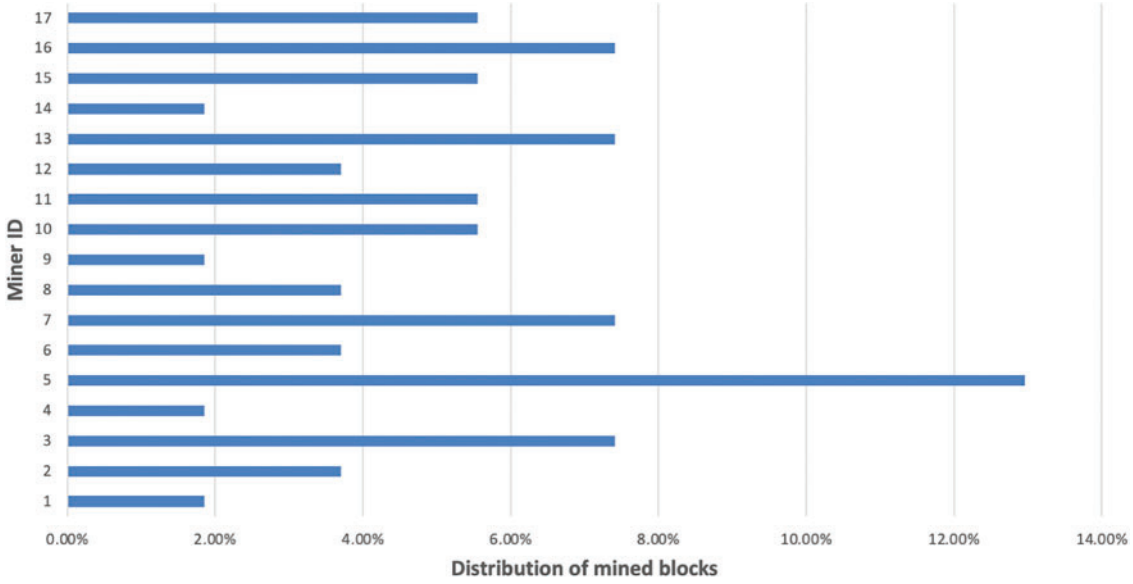

Figure 3: Average distribution of blocks mined by different miners (average across 3 trials)

4.3 Security Analysis

To assess the security robustness of the proposed model, we conducted tests to evaluate its resilience against a 51% attack. In this attack scenario, an adversary seeks to gain control over more than 51% of the total mining power within a single shard to establish dominance. To simulate this threat, we introduced adversary nodes with hashing power exceeding 50% of the shard's mining capacity in our model implementation. The experimentation involved varying the number of nodes as the independent variable while measuring the percentage of blocks mined by the attacker as the dependent variable. Other input parameters, such as block interval and block delay, remained consistent across all test runs. As depicted in Fig. 4, the attack was successful when there were only 5 nodes in a single shard. However, as the number of nodes increased, the percentage of blocks mined

by the adversary fell below 50%. Despite the attacker's dominance of over 50% of the mining power, the attack failed because it couldn't supersede the longest honest chain with the manipulated private attack chain. Based on these findings, it is recommended to have at least 10 miners participating in each block to maintain the robustness of the blockchain against a 51% attack.

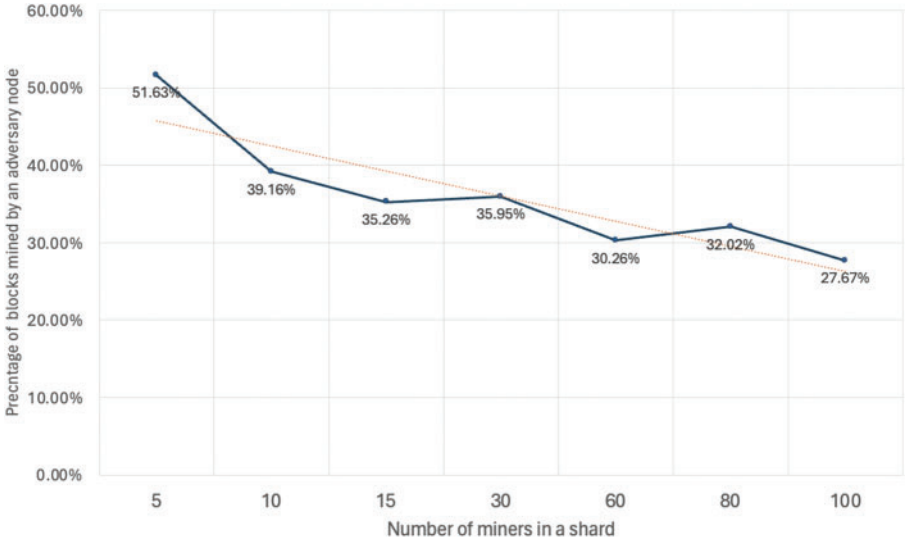

Figure 4: Security analysis of the proposed model against a 51% attack with variations in the number of miners

Another possible attack on blockchain is Sybil attacks involve a node using multiple deceptive nodes to seize control of the network. However, in the proposed model, such attacks are prohibitively expensive because the attacker needs numerous nodes with a genuine stake (cryptocurrency) to engage in the network, resulting in economic disincentives. Additionally, the network imposes penalties on nodes engaging in ma- licious behavior, potentially confiscating part or all their stake. Therefore, these factors act as deterrents for attackers in Sybil attack scenarios. The same preventive measures apply in a 51% attack scenario, the suggested hybrid model, which merges PoW and PoS, proves prohibitively expensive for executing such an attack. Additionally, the proposed model is robust to a double spending attack where a cryptocurrency can be used twice. To successfully execute a double spending attack in a hybrid PoW/PoS network, an attacker would need to overcome both the computational and economic barriers posed by PoW and PoS, respectively. This significantly increases the cost and complexity of carrying out such an attack, making it less feasible for attackers. Long-range attacks pose a significant threat to blockchain security, where an adversary creates an alternative blockchain fork from an earlier point in the chain, potentially overtaking the legitimate chain and causing a rollback [25]. This type of attack exploits the fact that, in some consensus mechanisms, older blocks are less secure and more susceptible to manipulation. The proposed model effectively counters long-range attacks using PoW in conjunction with PoS and enhances the security of historical blocks, as the high computational and stake requirements make it exceedingly difficult for an attacker to outpace the main chain.

Another potential security concern in blockchain is process starvation. Process starvation occurs when some nodes in a blockchain network are unable to participate effectively in the consensus process due to delays or excessive communication overhead. This issue often arises in consensus schemes like PBFT, where validation times increase with the number of nodes, leading to potential delays for some

nodes in participating fully. In comparison, our proposed shard-based hybrid consensus model, which integrates PoW and PoS, mitigates process starvation more effectively. By employing hierarchical shard levels and a dynamic PoS-based miner assignment, our model ensures that transactions are processed in parallel across multiple shards. This approach reduces communication overhead and latency, allowing for more equitable participation and minimizing the risk of process starvation. Thus, our model provides a more balanced and efficient solution compared to traditional schemes.

The comparison table (Tables 5 and 6) reveals that while traditional consensus schemes offer robust defenses against various blockchain attacks, they each have limitations. Issues such as process starvation and reduced decentralization are common, particularly in schemes that face high latency or computational imbalances. In contrast, our proposed shard-based hybrid consensus model improves upon these weaknesses by integrating mechanisms that enhance scalability, fairness, and overall security. This model effectively addresses attack vulnerabilities and mitigates risks associated with centralization and process starvation, making it a more resilient and efficient solution.

Table 5: Comparison of scalability, fairness, hardware requirements, and communication overhead across consensus schemes and the proposed model

Model	Scalability	Advanced hardware	Fair chance to participate	Communication overhead
PoW [26]	Low	Yes	Nodes with high power have higher chances of being selected	Low
PoS [15]	High	No	Nodes with high stakes have higher chances of being selected	Low
PoC [6]	High	No	Yes	Moderate
PBFT [5]	Low	No	Yes	High
PoSW (proposed model)	High	Yes, required for PoW	Yes, nodes with variant computational power have a chance to participate	Low

Table 6: Comparative analysis of security concerns between the proposed model and related works

Model	51% attack	Sybil attack	Double spending attack	Centralization	Long-range attack	Process starvation
PoW [26]	✓	✓	✓	✓	✓	×
PoS [15]	✓	✓	✓	×	×	×

(Continued)

Table 6 (continued)

Model	51% attack	Sybil attack	Double spending attack	Centralization	Long-range attack	Process starvation
PoC [6]	×	×	×	×	×	✓
PBFT [5]	✓	✓	✓	✓	✓	×
PoSW (proposed model)	✓	✓	✓	✓	✓	✓

4.4 Comparison with Other Consensus Methods

To assess the significance of the current study, the proposed model (PoSW) has been evaluated against four established consensus methods across six criteria: Scalability, Resistance to 51% attacks, Hardware requirements, Centralization tendency, Equal opportunity for participation, and Communication overhead. As seen from Table 5, in terms of scalability, the hybrid model surpasses consensus methods like PoW and PBFT [27] due to the incorporation of sharding [28]. Sharding allows multiple shards to work on transactions in parallel which increases the throughput of the network as proved by the results in Table 3. Furthermore, as previously discussed in the security analysis section, the proposed model demonstrates resilience against 51% attacks and Sybil attacks, attributed to its complexity and the economic barriers necessary to execute such attacks. This stands in contrast to PBFT, PoS, and PoC, which are susceptible to these types of attacks [27]. In terms of hardware requirements, the proposed model PoSW necessitates advanced hardware owing to the incorporation of the PoW algorithm, which demands high computational power to find the required nonce. Given the pursuit of enhanced decentralization in blockchain technology, it's crucial to consider this aspect when selecting the optimal consensus algorithm. With PoW, PoS, and PBFT, the risk of centralization is present, whereas in the proposed model, it is mitigated due to sharding, allowing each shard to autonomously process its own transactions. Additionally, in a public blockchain, ensuring that participants have a fair opportunity to participate is crucial for reducing the risk of centralization. In the proposed model, there are three levels of shards (the number of which can be adjusted based on network requirements) tailored to accommodate participants with varying computational power and stake. This approach provides a better chance of participation compared to, for example—PoW, where all participants compete against each other regardless of differences in computational power which gives a better chance for participants with high computational powers.

The comparison between the proposed model and the Monoxide sharding technique [4] reveals significant distinctions. As detailed in Section 2, the Monoxide sharding algorithm randomly assigns miners to shards. In contrast, our proposed model employs a methodology that leverages Proof of Stake and miners' hash power for shard allocation. Rather than random assignment, miners are allocated to shards based on predefined thresholds. Consequently, our model achieves a more efficient division of miners across shards. By organizing miners according to their computational power, the proposed model fosters collaboration among miners with similar capabilities within the same shard. This approach enhances fairness and optimizes the mining possibilities across the network.

To evaluate the effectiveness of the PoSW miner assignment method, an experiment was done with the following configuration: 10 miners were assigned to three shard levels according to their stake and hash power. In this experiment, we quantified the total number of blocks mined by each shard. As illustrated in Fig. 5, the shard with high computational power miners demonstrated faster block mining compared to the mid and low shards. Moreover, hierarchical assignment exhibited more coherent and distinguishable performance compared to random assignment. Random assignment of miners to zones can result in uneven distribution of resources across shards. For this reason, the proposed model aims to address this issue by considering the computational power of each miner when assigning them to shards. This performance variation can be utilized to prioritize specific transactions requiring faster processing. For instance, urgent transactions (and those ready to pay higher transaction fees) can be assigned to the high shard, given its higher throughput compared to the other shards. Finally, the proposed PoSW model results in minimal communication overhead compared to the PBFT algorithm. In PoSW, participants within a single shard autonomously process their own transactions, reducing the need for extensive communication.

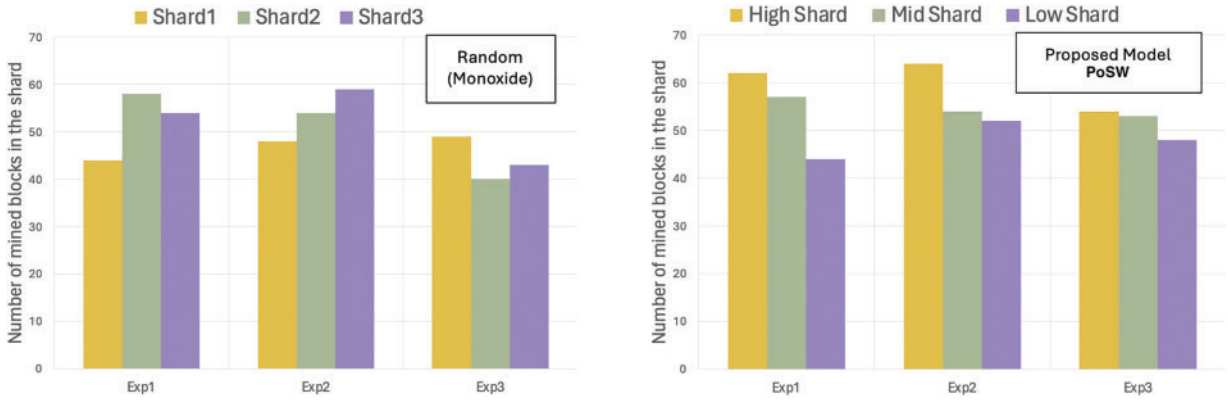

Figure 5: Comparison between two methods of assigning miners to shards: Monoxide sharding [4] and our proposed model PoSW

5 Conclusion

In this research, we proposed a shard-based hybrid consensus mechanism, PoSW, which integrates Proof of Work (PoW) and Proof of Stake (PoS) to overcome the inherent limitations of traditional consensus algorithms in blockchain systems. Our approach effectively addresses the scalability issues of PoW and the monopolization risks of PoS by leveraging sharding for parallel transaction processing and combining the strengths of both consensus methods. Through the integration of sharding, the system is able to achieve higher throughput and lower latency, while ensuring fairness in miner participation and maintaining the security of the network. We evaluated the performance and security of the proposed PoSW model against established consensus mechanisms such as Monoxide and Practical Byzantine Fault Tolerance (PBFT). The experimental results demonstrated that PoSW not only improves resource utilization compared to Monoxide but also reduces communication overhead when compared to PBFT, primarily due to the efficient use of PoW in the hybrid design. Moreover, the security analysis confirmed that PoSW provides robust protection against well-known blockchain vulnerabilities, including the 51% attack and Sybil attack, thereby enhancing the resilience of the system. By addressing the scalability, security, and fairness challenges faced by existing blockchain systems, the PoSW mechanism offers a promising solution for decentralized environments that demand high

performance and resilience. Future work will focus on optimizing cross-shard communication and exploring further enhancements to the fault tolerance mechanisms to ensure smooth operation in even larger-scale blockchain networks. Additionally, we plan to explore the potential of PoSW in other domains and applications, expanding its applicability to various decentralized systems.

Acknowledgement: The authors would like to express their gratitude to Dr. Mohammad Shorfuzzaman, Department of Computer Science, Taif University, Saudi Arabia for his advice during this research.

Funding Statement: No funding was received for this work.

Author Contributions: The authors confirm their contribution to the paper as follows: Study Conception and Design: Hind Baageel, Md Mahfuzur Rahman; Data Collection, Experiment and Analysis: Hind Baageel; Supervision, Discussion: Md Mahfuzur Rahman; Writing, Editing, Reviewing: Hind Baageel, Md Mahfuzur Rahman. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data is available upon request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] V. Kustov, N. Beksaev, and R. Ravi, "The blockchain SSD trilemma or chasing three birds with one stone," presented at the 16th Int. Conf. Adv. Technol., Syst., Serv. in Telecommun. (TELSIKS), Serbia, 2023, pp. 219–222.

[2] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang and R. P. Liu, "Survey: Sharding in blockchains," *IEEE Access*, vol. 8, pp. 14155–14181, 2020.

[3] D. Yu, H. Xu, L. Zhang, B. Cao, and M. Imran, "Security analysis of sharding in the blockchain system," presented at the IEEE 32nd Annu. Int. Symp. on Pers., Indoor, Mobile Radio Commun. (PIMRC), Helsinki, Finland, IEEE, 2021, pp. 1030–1035.

[4] J. Wang and H. Wang, "Monoxide: Scale-out blockchain with asynchronous consensus zones," in *Proc. 16th USENIX Conf. Netw. Syst. Design and Implementation, NSDI'19*, USA, 2019, pp. 95–112.

[5] B. Yuan, H. Jin, D. Zou, L. T. Yang, and S. Yu, "A practical byzantine-based approach for faulty switch tolerance in software-defined networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 15, pp. 825–839, 2018. doi: 10.1109/TNSM.2018.2822668.

[6] H. Song, N. Zhu, R. Xue, J. He, K. Zhang and J. Wang, "Proof-of-contribution consensus mechanism for blockchain and its application in intellectual property protection," *Inf. Process. Manage.*, vol. 58, no. 3, 2021. doi: 10.1016/j.ipm.2021.102507.

[7] M. A. Manolache, S. Manolache, and N. Tapus, "Decision making using the blockchain proof of authority consensus," *Procedia Comput. Sci.*, vol. 199, pp. 580–588, 2022. doi: 10.1016/j.procs.2022.01.071.

[8] A. Rosli, S. Hassan, and M. H. Omar, "Data authentication mechanism using blockchain's proof-of-trust mechanism in named data networking," in *Proc. 2nd Int. Recent Trends Eng., Adv. Comput. and Technol. Conf.*, Perth, Australia, 2023.

[9] S. Masseport, B. Darties, R. Giroudeau, and J. Lartigau, "Proof of Experience: Empowering proof of work protocol with miner previous work," presented at the 2nd Conf. Blockchain Res. Appl. for Innov. Netw. and Serv. (BRAINS), Paris, France, 2020, pp. 57–58.

[10] A. Endurthi and A. Khare, "Two-tiered consensus mechanism based on proof of work and proof of stake," presented at the 9th Int. Conf. Comput. for Sustain. Glob. Dev. (INDIACom), New Delhi, India, 2022, pp. 349–353.
[11] G. Praveen, S. P. Singh, V. Chamola, and M. Guizani, "Novel consensus algorithm for blockchain using proof-of-majority (PoM)," *IEEE Netw. Lett.*, vol. 4, no. 10, pp. 208–211, 2022.
[12] K. Karantias, A. Kiayias, and D. Zindros, "Proof-of-burn. In financial cryptography and data security," presented at the 24th Int. Conf., Malaysia, 2020, pp. 523–540.
[13] Z. Hussein, M. Salama, and S. El-Rahman, "Evolution of blockchain consensus algorithms: A review on the latest milestones of blockchain consensus algorithms," *Cybersecurity*, vol. 6, no. 1, 2023, Art no. 30. doi: 10.1186/s42400-023-00163-y.
[14] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Appl. Sci.*, vol. 9, no. 9, 2019, Art. no. 1788.
[15] Y. Gao, S. Kawai, and H. Nobuhara, "Scalable blockchain protocol based on proof of stake and sharding," *J. Adv. Comput. Intell. Intell. Informat.*, vol. 23, no. 9, pp. 856–863, 2019.
[16] X. Huang, H. Yin, Y. Wang, Q. Chen, and J. Zhang, "Location-based reliable sharding in blockchain-enabled fog computing networks," presented at the 2022 14th Int. Conf. Wireless Commun. Signal Process. (WCSP), Nanjing, China, 2022, pp. 12–16.
[17] J. Xi *et al.*, "A blockchain dynamic sharding scheme based on hidden Markov model in collaborative IoT," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14896–14907, 2023. doi: 10.1109/JIOT.2023.3294234.
[18] F. Rahman, C. Titouna, and F. Nait-Abdesselam, "Prioritised sharding: A novel approach to enhance blockchain scalability," presented at the 2023 5th Conf. Blockchain Res. Appl. for Innov. Netw. Serv. (BRAINS), Paris, France, 2023, pp. 1–2.
[19] H. Huang, Q. Zhao, and X. Ran, "Secure sharding scheme of blockchain-based on reputation," presented at the IEEE 2nd Int. Conf. Data Sci. Comput. Appl. (ICDSCA), Dalian, China, 2022, pp. 1324–1327.
[20] P. Zheng, Q. Xu, Z. Zheng, Z. Zhou, Y. Yan and H. Zhang, "Meepo: Sharded consortium blockchain," presented at the 2021 IEEE 37th Int. Conf. Data Eng. (ICDE), Chania, Greece, 2021, pp. 1847–1852.
[21] K. Vinodha, R. Jayashree, G. Kommineni, M. Tanna, and G. P. Prerna, "Sharding in blockchain systems: Concepts and challenges," presented at the 2022 Int. Conf. Smart Generation Comput., Commun. Netw. (SMART GENCON), Bangalore, India, 2022, pp. 1–7.
[22] E. Kokoris-Kogias *et al.*, "OmniLedger: A secure, scale-out, decentralized ledger via sharding," in *2018 IEEE Symp. Security and Privacy (SP)*, San Francisco, CA, USA, 2018, pp. 583–598.
[23] M. Alharby and A. van Moorsel, "BlockSim: An extensible simulation tool for blockchain systems," *Front. Blockchain*, vol. 3, 2020, Art. no. 28.
[24] A. Hafid, A. S. Hafid, and D. Makrakis, "Sharding-based proof-of-stake blockchain protocols: Key components and probabilistic security analysis," *Sensors*, vol. 23, no. 5, 2023, Art. no. 2819.
[25] O. Sanda, M. Pavlidis, S. Seraj, and N. Polatidis, "Long-range attack detection on permissionless blockchains using deep learning," *Expert. Syst. Appl.*, vol. 218, no. 5, 2023, Art. no. 119606. doi: 10.1016/j.eswa.2023.119606.
[26] M. J. Bsson and A. Juels, "Proofs of work and bread pudding protocols," in *Secure Information Networks. IFIP—The International Federation for Information Processing*, USA: Springer, 1999, vol. 23, pp. 258–272.
[27] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: Challenges and solutions," *Blockchain: Res. Appl.*, vol. 2, no. 2, 2021, Art. no. 100006.
[28] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE Access*, vol. 8, pp. 125244–125262, 2020.