I.J. Wireless and Microwave Technologies, **2023, 5, 11-22**
Published Online on October 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2023.05.02

A Secure Network for Streamlined and High-Performance Consensus Algorithm based on Blockchain Technology

Deven A Gol*
Ph.D. Research Scholar, Computer Science Engineering, The CVM University, Anand, Gujarat 388120, India
E-mail: deven215@gmail.com
ORCID iD: https://orcid.org/0000-0002-8258-3945
*Corresponding Author

Nikhil Gondaliya
Ph.D. Supervisor, Computer/IT Engineering, The CVM University
Associate Professor, Department of Information Technology, GCET Engineering College, V.V. Nagar, Anand, Gujarat 388120, India
Email: nikhilgondaliya@gcet.ac.in
ORCID iD: https://orcid.org/0000-0001-7011-5469

Received: 22 February, 2023; Revised: 05 April, 2023; Accepted: 20 May, 2023; Published: 08 October, 2023

Abstract: The blockchain technology has been widely adopted for various applications due to its decentralization, transparency, and security features. Consensus algorithms, such as Proof of Work (PoW) and Proof of Stake (PoS), are fundamental components of blockchain technology, ensuring the integrity and validity of the blockchain network. However, the current consensus algorithms face challenges such as scalability, energy consumption, and security threats. To address these challenges, a new secure network for streamlined and high-performance consensus algorithm based on blockchain technology has been proposed. This new network incorporates the advantages of PoW and PoS, resulting in a hybrid consensus algorithm that is more efficient and secure than the existing algorithms. Additionally, the new network utilizes a dynamic sharding mechanism to improve scalability, reducing the overall processing time of transactions. The simulation results help identify potential vulnerabilities and inefficiencies in the consensus algorithm. Optimal combinations of block interval and propagation delay are determined based on specific use cases, balancing high throughput with security and consensus stability. The study also validates the security of Proof-of-Work (PoW) by comparing the fraction of generated blocks with the expected blocks based on miners' hashing power. This study establishes a foundation for future improvements in consensus algorithms, contributing to their evolution and facilitating the implementation of blockchain applications in various domains such as finance, healthcare, supply chain management, and more. The proposed solution aims to provide a more robust and efficient blockchain platform that can handle a higher volume of transactions while maintaining its security features.

Index Terms: Lightning Network, 51% attack, Streamlined and High-Performance Consensus Algorithm (SHP), Blockchain, Consensus Mechanism.

1. Background on Blockchain Technology and Consensus Algorithms

Blockchain technology is a decentralized and secure method of recording transactions. It consists of a network of computers, or nodes, that validate and store transactions in a decentralized manner. This means that there is no central authority controlling the network, and each node has a copy of the blockchain ledger. Blockchain technology is transparent, meaning that anyone can view the transactions on the network, and it is immutable, meaning that once a transaction is added to the blockchain, it cannot be altered. Consensus algorithms are the backbone of the blockchain technology, ensuring the integrity and validity of the network.[1] In a blockchain network, each node is responsible for validating and verifying transactions. Consensus algorithms are used to reach agreement among nodes about the state of the network and the order in which transactions are added to the blockchain. There are several consensus algorithms used in blockchain technology, including Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS)[2-13]. PoW requires nodes to solve complex mathematical problems to validate transactions, while PoS requires nodes to hold a certain amount of cryptocurrency to validate transactions. DPoS allows for the delegation of

validation power to trusted parties. Each of these consensus algorithms has its own advantages and disadvantages, and their effectiveness depends on the specific use case. However, the current consensus algorithms face challenges such as scalability, energy consumption, and security threats. The scalability issue arises because the current consensus algorithms require all nodes to validate all transactions, leading to a bottleneck in the network's processing capacity[14]. To improve scalability, the solution incorporates modifications such as sharding, which divides the blockchain network into smaller partitions called shards. This allows for parallel processing of transactions, significantly increasing the network's capacity to handle a higher volume of transactions. The energy consumption issue arises because PoW requires nodes to solve complex mathematical problems, which consume a significant amount of energy. In terms of performance, the solution employs optimization techniques, including off-chain transactions and a layered architecture. Off-chain transactions enable certain transactions to be conducted outside the main blockchain, reducing the overall load on the network. This enhances performance by minimizing the number of transactions that need to be processed on the main chain. Finally, security threats arise because malicious nodes can manipulate the network by controlling the majority of the network's computing power. This involves real-time monitoring of network activities, analyzing anomalies, and taking proactive measures to protect the network's security. To address these challenges[15-32], a new secure network for streamlined and high-performance consensus algorithm based on blockchain technology has been proposed. The proposed solution aims to enhance the robustness and efficiency of the blockchain platform by addressing scalability, performance, and lightweight consensus mechanisms. It achieves this through modifications to key parameters within the agreement protocol and optimizing the voting system for faster results. The research background highlights the decentralized and secure nature of blockchain technology, along with its consensus algorithms and the challenges it faces in terms of scalability, energy consumption, and security threats.

A. Motivation

The motivation for developing a secure network for streamlined and high-performance consensus algorithm based on blockchain technology arises from the challenges faced by the existing consensus algorithms. The current consensus algorithms, such as PoW and PoS, are facing scalability, energy consumption, and security challenges. Scalability[33] is a significant challenge for blockchain technology. The current consensus algorithms require all nodes to validate all transactions, leading to a bottleneck in the network's processing capacity. This leads to slow processing times and high fees for users. Additionally, as the number of transactions on the network increases, the size of the blockchain ledger grows, making it difficult for nodes to store and process the data. Energy consumption[11] is another challenge for blockchain technology. PoW requires nodes to solve complex mathematical problems to validate transactions, which consume a significant amount of energy. This has raised concerns about the environmental impact of blockchain technology, and the high energy consumption has made it difficult for blockchain technology to be adopted on a larger scale. Finally, Security threats[34] are a significant challenge for blockchain technology. Malicious nodes can manipulate the network by controlling most of the network's computing power. This is known as the 51% attack, where a single entity controls more than 50% of the network's computing power. This can lead to double spending, where a user spends the same cryptocurrency twice. Currently, there is a lack of existing solutions in the blockchain industry for this specific application. However, there have been a few proposed works and some cryptocurrency-based solutions available[3]. To address these challenges, a new secure network for streamlined and high-performance consensus algorithm based on blockchain technology has been proposed.

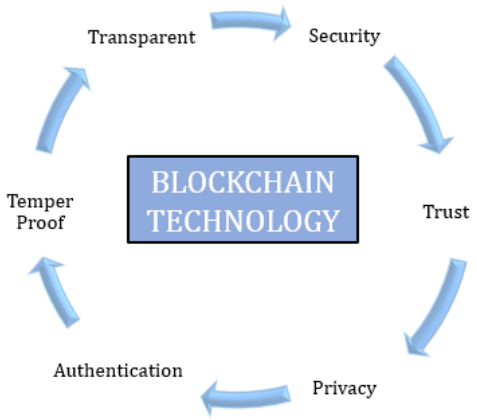

Fig. 1. The Pillars of blockchain

The proposed solution aims to enhance the efficiency and security of blockchain platforms, enabling them to process a larger number of transactions without compromising security. This advancement has the potential to transform industries by fully harnessing the power of blockchain technology. In terms of societal impact, the improved efficiency and scalability of the blockchain network can facilitate faster and more seamless transactions. This can lead to enhanced financial inclusion, as more individuals and businesses can access secure and efficient digital transactions.

It can also streamline processes in various industries such as supply chain management, healthcare, and government services, resulting in improved transparency, accountability, and reduced costs. Moreover, the increased security features of the blockchain platform can help mitigate the risks of fraud, data manipulation, and unauthorized access. This can enhance trust and confidence in digital transactions, fostering a more secure and reliable digital ecosystem. The objective of the proposed solution is to address these challenges and enhance the robustness, efficiency, and performance of the blockchain platform through modifications to the agreement protocol and voting system.

2. The Revised Approach

The research proposes a new secure network that addresses the challenges faced by existing consensus algorithms. The proposed network incorporates the advantages of both PoW and PoS, resulting in a hybrid consensus algorithm that is more efficient and secure than the existing algorithms. The new network also utilizes a dynamic sharding mechanism to improve scalability and a Byzantine fault-tolerant (BFT) consensus algorithm to enhance security[35-40]. This approach aims to achieve a balance between energy efficiency, security, and decentralization within the network. The paper introduces a novel strategy for reducing energy consumption while preserving the network's security and decentralized nature with help of different parameter modifications in blockchain consensus mechanism. The sharding mechanism partitions the network into smaller sub-networks called shards, enabling simultaneous processing of transactions. As a result, scalability is improved, and the overall transaction processing time is reduced[42]. To bolster security, the network incorporates fundamental principles from a Byzantine Fault Tolerant (BFT) consensus algorithm. This algorithm ensures that the network can withstand malicious attacks from rogue nodes. Even in scenarios where a certain number of nodes are compromised, the BFT consensus algorithm guarantees that the network can still reach a consensus. Consequently, it provides a high level of security even when nodes fail within the network[18]. The POW blockchain network has the potential to provide a more robust and efficient blockchain platform that can handle a higher volume of transactions while maintaining its security features. Proof-of-Work (PoW) is a consensus algorithm used by many blockchain networks to validate transactions and create new blocks. While it has been successful in securing the Bitcoin network, it has some drawbacks, such as high energy consumption and low transaction throughput[41].

A. Advancements in the Proof-of-Work Consensus Algorithm: Enhancing Efficiency and Security

- **Proportional hashing power:** In traditional PoW, the node with the most hashing power has the highest chance of creating a new block[42]. However, this creates an unfair advantage for large miners and leads to centralization. A better approach would be to proportionally distribute the chances of creating a new block based on a miner's hashing power, which would incentivize smaller miners to join the network.
- **Dynamic block difficulty:** The difficulty of creating a new block in PoW is set based on the total hashing power of the network, which can make it too difficult for small miners and too easy for large miners. A better approach would be to dynamically adjust the block difficulty based on the number of miners on the network, making it more challenging when there are more miners and easier when there are fewer miners[43].
- **Proof-of-stake hybrid:** PoW requires a lot of computational power, which leads to high energy consumption. A proof-of-stake (PoS) hybrid approach could reduce the energy consumption by allowing nodes to validate blocks based on the amount of cryptocurrency they hold rather than the computational power they provide[14]. This would make it easier for smaller miners to participate and incentivize holding the cryptocurrency, but it also has some drawbacks such as potential centralization around wealthy stakeholders.
- **Two-factor consensus:** A potential way to reduce the risk of a 51% attack, where a single entity controls more than half of the network's computational power, would be to require two forms of consensus[40]. For example, a block could only be added to the chain if it is approved by a certain percentage of nodes and also validated by a certain percentage of cryptocurrency holders.
- **Resource-friendly alternatives:** Another potential way to reduce energy consumption and environmental impact could be to develop consensus mechanisms that do not rely on intensive computation or require energy-intensive hardware. Some examples of such consensus mechanisms include Proof-of-Authority, Proof-of-Elapsed-Time, or Proof-of-Identity[41–47]. However, these alternatives may have their own drawbacks in terms of security and decentralization.

The paper highlights the importance of addressing the challenges faced by existing consensus algorithms and proposes a solution that can significantly improve the efficiency and security of blockchain technology.

3. Key Considerations in Designing a Consensus Algorithm: A Methodological Approach

Designing a consensus algorithm is a complex task that requires careful consideration of several factors, including scalability, security, energy consumption, and decentralization.

A. Key steps to consider when designing a consensus algorithm

- The requirements: The first step in designing a consensus algorithm is to determine the requirements of the network based on the nature of the industry problem. This includes considering factors such as the number of nodes involved in the network, the expected transaction volume, the desired level of security to protect sensitive data, and the energy efficiency goals to ensure environmental sustainability. By understanding these requirements, the consensus algorithm can be tailored to meet the specific needs of the industry and optimize its performance accordingly.
- A consensus model: There are several consensus models available, including Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Byzantine Fault Tolerance (BFT). Each model has its own set of advantages and disadvantages, and the choice of consensus model depends on the specific requirements of the network, which will be discussed in detail later in this research work. For the purpose of this study, the chosen base consensus model is Proof of Work (PoW) due to its streamlined and high-performance characteristics. Once the base consensus model is selected, the next step is to define the consensus mechanism, which involves establishing the rules for validating transactions, designing the reward system, and implementing a penalty system to address malicious nodes.
- A mechanism for selecting validators: In a Proof of Stake (PoS) or Delegated Proof of Stake (DPoS) consensus algorithm, nodes are typically selected to validate transactions based on the amount of cryptocurrency they hold. This mechanism ensures that nodes with a higher stake have a greater chance of being chosen as validators. However, in this research work, a minor modification has been introduced to the PoS algorithm by incorporating elements of the bitcoin reward system. The goal of this modification is to enhance the performance of the Proof of Work (PoW) mechanism. By combining aspects of both PoS and PoW, the aim is to create an improved version of the consensus mechanism, taking advantage of the benefits offered by each approach. This approach seeks to enhance the efficiency, security, and decentralization of the consensus algorithm in achieving consensus within the network.
- The network topology: The network topology plays a crucial role in the structure of the blockchain network. It encompasses factors such as the number of nodes involved and their connectivity, which contribute to the overall environment for the blockchain. When designing the network topology, it is important to prioritize aspects such as security, scalability, and decentralization. By carefully considering these factors, the network topology can be optimized to provide a robust and efficient infrastructure for the blockchain, ensuring secure and scalable operations while maintaining a decentralized nature.
- The block structure: The block structure defines the format of the blocks added to the blockchain, including the transaction data, the timestamp, and the proof of work or stake.
- The fork resolution mechanism: In a decentralized network, there may be multiple valid versions of the blockchain. A fork resolution mechanism is necessary to determine the valid version of the blockchain and prevent double spending.
- Test and optimize the consensus algorithm: The final step in designing a consensus algorithm is to test and optimize it for efficiency, security, and scalability.

The research paper highlights the critical factors involved in designing a consensus algorithm, encompassing scalability, security, energy consumption, and decentralization. In this work, we have demonstrated the significance of achieving a delicate balance among these factors to construct a robust and efficient consensus algorithm. This algorithm is designed to effectively address the evolving demands of a growing blockchain network.

4. Literature Survey on Blockchain Consensus Algorithms

Blockchain consensus algorithms are at the heart of every blockchain network, and they are responsible for ensuring that the network remains secure, decentralized, and tamper-proof. Over the years, several consensus algorithms have been proposed, each with its own strengths and weaknesses. In this literature survey[25–31], we will delve into a comprehensive analysis of some of the most widely used and influential blockchain consensus algorithms. By examining their principles, mechanisms, and performance, we aim to gain insights into the diverse approaches employed to achieve consensus in blockchain networks.

Table 1 presents a summary of several popular blockchain consensus algorithms, providing a convenient comparison of different approaches along with their respective advantages and limitations [48-51]. In summary, Proof of Work (PoW) is known for its decentralized and secure nature, but it comes with drawbacks such as high energy consumption and slow transaction speed. Proof of Stake (PoS) offers energy efficiency and fast transaction processing, but it carries risks of centralization and implementation challenges. Delegated Proof of Stake (DPoS) emphasizes speed and scalability but faces concerns related to centralization and limited participation. Practical Byzantine Fault Tolerance (PBFT) ensures fast transaction finality but may encounter scalability limitations and centralization risks. Honey Badger Byzantine Fault Tolerance (HBBFT) exhibits high throughput and robustness, though its adoption may be limited due to

complex implementation. Avalanche is a newer consensus algorithm, offering fast, scalable, and adaptive properties, but it requires further testing and validation due to its relative novelty.

Table 1. Comparing Consensus Algorithms: Assessing Merits and Demerits

Consensus Algorithm	Research Paper	Advantages	Limitations
Proof of Work (PoW)	Nakamoto, S. (2008)	Decentralized, Secure	High energy consumption, slow
Proof of Stake (PoS)	King, S., & Nadal, J. (2012)	Energy-efficient, Fast	Centralization risk, difficult implementation
Delegated Proof of Stake (DPoS)	Larimer, D. (2014)	Fast, Scalable	Centralization risk, limited participation
Practical Byzantine Fault Tolerance (PBFT)	Castro, M., & Liskov, B. (1999)	Fast, Finality	Centralization risk, limited scalability
Honey Badger Byzantine Fault Tolerance (HBBFT)	Miller, A., Xia, Y., Croman, K., & Shi, E. (2016)	High throughput, Robustness	Complex implementation, limited adoption
Avalanche	Team Rocket (2018)	Fast, Scalable, Adaptive	New, not widely tested

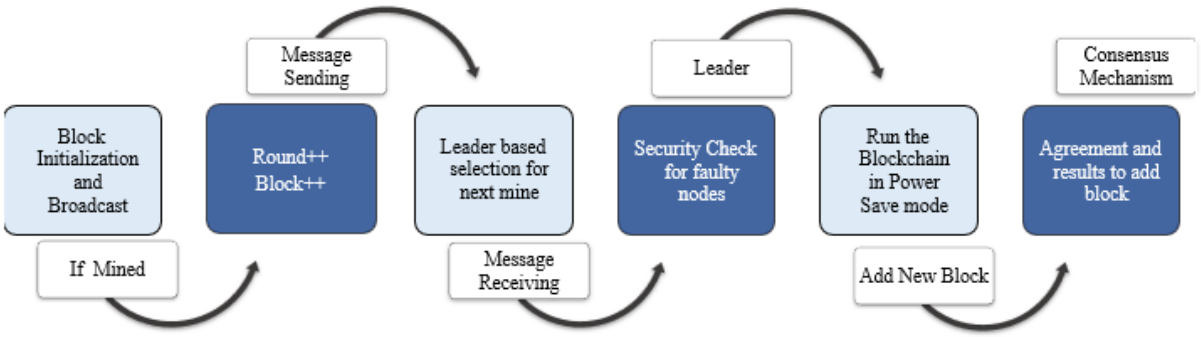

Fig. 2. Optimizing Existing Blockchain Protocols to Enhanced Performance and Security

There have been studies and research papers have been published on the Proof of Work (PoW) algorithm, delving into various aspects of its design, implementation, and performance. The accompanying table 2 presents a survey of the Proof of Work (PoW) consensus algorithm, showcasing important parameters for evaluating its performance and addressing research gaps.

Table 2. Literature Survey of Consensus Algorithm Features

Feature	Description	Status	Year	Application	Importance
Optimized Mining Algorithms	Use of more efficient mining algorithms to reduce energy consumption	Implemented	2014	Cryptocurrencies (Bitcoin, Litecoin)	High
Faster Block Times	Reduction in block creation time to improve confirmation times	Implemented	2016	Cryptocurrencies (Litecoin, Ethereum)	High
Parallel Processing	Ability to process multiple transactions simultaneously to improve confirmation times	Implemented	2018	Cryptocurrencies (Ethereum, Bitcoin Cash)	High
Mining Difficulty Adjustment	Mechanisms to adjust mining difficulty to prevent centralization	Implemented	2009	Cryptocurrencies (Bitcoin, Litecoin)	High
Randomized Mining Rewards	Randomized reward distribution to incentivize smaller mining operations	In development	N/A	Cryptocurrencies (TBD)	Medium
Adaptive Mining Algorithm	An algorithm that can adapt to changing network conditions to improve security and reduce energy consumption	In development	N/A	Cryptocurrencies (TBD)	High
Merkle Trees for Efficient Verification	Use of Merkle Trees to improve transaction verification efficiency	Implemented	2011	Cryptocurrencies (Bitcoin, Ethereum)	Medium
Proof of Work with Proof of Stake Hybrid Consensus	Combination of PoW and PoS to reduce energy consumption and increase security	In development	N/A	Cryptocurrencies (Ethereum 2.0, TBD)	High
Sustainable Mining Practices	Use of alternative energy sources and more sustainable mining practices to reduce carbon emissions	In development	N/A	Cryptocurrencies (TBD)	High

Reduced Energy Consumption	Implementation of more efficient mining algorithms and hardware to reduce energy consumption.	Ongoing	N/A	Public and private blockchains	High
Interoperability	The ability for different blockchain networks to communicate and share information with each other.	In development	N/A	Public and private blockchains	High
Sharding	Breaking up the blockchain into smaller, more manageable pieces to improve scalability and increase transaction throughput.	In development	N/A	Public and private blockchains	High
Smart Contract Functionality	Ability to execute complex business logic and automate processes through the use of smart contracts.	Implemented	2015	Public and private blockchains	High
Privacy and Confidentiality	The ability to keep sensitive information private and confidential through advanced cryptographic techniques such as zero-knowledge proofs.	In development	N/A	Private and consortium blockchains	High

This literature study provides an overview of key research areas focused on optimizing the PoW consensus algorithm and addressing existing research gaps. The aim of this study is to identify opportunities for improvement and propose innovative solutions to enhance the efficiency, scalability, and security of PoW-based blockchain systems [16-55]. By analyzing the existing literature, this research aims to contribute to the advancement of PoW algorithms and provide valuable insights for future research and development in this domain.

5. Implementation of Consensus Algorithm in Blockchain: Design and Security Considerations

The consensus algorithm plays a critical role in the functioning of a blockchain network. It is responsible for ensuring that all nodes in the network agree on the current state of the blockchain and that new transactions are added to the chain in a secure and tamper-proof manner. When a new transaction is initiated on the network, it is first broadcast to all nodes in the network. These nodes will then validate the transaction to ensure that it meets certain criteria, such as having the correct format and adhering to any rules set by the network[48-51]. Once a sufficient node has validated the transaction, it is added to a pool of unconfirmed transactions. The next step is to add the transaction to a block. A block is a bundle of transactions that have been confirmed and added to the blockchain. Before a block can be added to the blockchain, it must be verified by the consensus algorithm. This involves a process called mining, which is carried out by nodes known as miners. In a proof-of-work (PoW) consensus algorithm, miners compete to solve a complex mathematical problem. The first miner to solve the problem and validate the block is rewarded with a set amount of cryptocurrency. The other nodes in the network then validate the block to ensure that it meets the network's rules and add it to their local copy of the blockchain. In a proof-of-stake (PoS) consensus algorithm, nodes are selected to validate blocks based on the amount of cryptocurrency they hold. The more cryptocurrency a node holds, the more likely it is to be selected as a validator. Once a validator has been selected, they must verify the block and add it to the blockchain. Once a block has been added to the blockchain, it is considered immutable and cannot be altered without also altering all subsequent blocks. This makes the blockchain network highly secure and resistant to tampering or fraudulent activity[25-27]. In summary, the consensus algorithm ensures that all nodes in a blockchain network agree on the current state of the blockchain and that new transactions are added to the chain in a secure and tamper-proof manner. This is achieved through a process of validation and mining, which is carried out by nodes in the network.

A. Understanding Security Threats to Blockchain Networks: Overview and Analysis of Common Attacks and Vulnerabilities

Blockchain networks are designed to be decentralized, transparent, and secure. However, they are not completely immune to attacks. Here are some common attacks on blockchain networks, specifically those that use a proof-of-work (PoW) consensus algorithm:

- **51% Attack:** This attack occurs when a single entity or group controls more than 50% of the network's computing power. With this control, the attacker can manipulate the blockchain by rejecting valid transactions, double-spending coins, and rewriting the blockchain's history.
- **Double-Spending:** In a double-spending attack, an attacker attempts to spend the same cryptocurrency twice by creating two conflicting transactions. To execute this attack, the attacker must control enough computing power to mine two blocks simultaneously, creating two different versions of the blockchain. The attacker can then broadcast one version of the blockchain to some nodes, and the other version to other nodes. If the attacker's chain is longer, it will be considered the valid one, and the double-spending will be successful.

- **Selfish Mining:** In a selfish mining attack, a miner or group of miners withhold newly mined blocks from the network, hoping to mine additional blocks before revealing their new chain to the network. This gives the selfish miner a head start in the mining race and allows them to earn more rewards than they would otherwise.
- **Sybil Attack:** A Sybil attack occurs when an attacker creates multiple fake identities to control a significant portion of the network. By doing so, they can gain influence and manipulate the network's decisions, such as censoring certain transactions or controlling which blocks are added to the blockchain.
- **Eclipse Attack:** In an eclipse attack, the attacker isolates a particular node in the network by surrounding it with their own nodes. By doing so, they can prevent the isolated node from receiving new transactions and can manipulate the transactions it broadcasts to the network.

These are just a few examples of common attacks on blockchain networks that use a proof-of-work consensus algorithm[36–45]. To combat these attacks, blockchain networks often have built-in defenses, such as network-wide consensus mechanisms, decentralized governance structures, and cryptographic techniques to secure the transactions and the blockchain's integrity.

B. Enhancing Security and Resilience of Blockchain Networks: Mitigating Common Attacks and Vulnerabilities

Improving the security of blockchain networks is an ongoing process, as new attack vectors and vulnerabilities can emerge over time. Here are some ways in which common attacks on proof-of-work (PoW) based blockchain networks can be improved:

- **51% Attack Improvement:** One way to improve the prevention of 51% attacks is to implement more secure consensus algorithms, such as proof-of-stake (PoS) or delegated proof-of-stake (DPoS). These algorithms use different mechanisms to prevent malicious actors from controlling the network's computing power, such as requiring nodes to hold a certain amount of cryptocurrency or assigning validation responsibilities to a select group of trusted nodes.
- **Sybil Attack Improvement:** To improve protection against Sybil attacks, blockchain networks can use identity verification mechanisms, such as digital signatures or biometric authentication, to ensure that nodes are authentic and not fake identities created by malicious actors.
- **Double Spending Improvement:** To improve the prevention of double spending, blockchain networks can implement faster transaction confirmation times, which reduces the window of opportunity for malicious actors to double spend. Additionally, new consensus algorithms, such as Byzantine Fault Tolerance (BFT), can offer stronger protection against double spending.
- **Selfish Mining Improvement:** To improve protection against selfish mining, blockchain networks can use improved mining algorithms, such as Equihash, which are designed to be resistant to selfish mining. Additionally, delayed broadcast mechanisms or other methods that prevent miners from gaining an unfair advantage can be used to improve protection against selfish mining.
- **Eclipse Attack Improvement:** To improve protection against eclipse attacks, blockchain networks can implement more robust peer-to-peer networking protocols that prevent nodes from being isolated from the rest of the network. Additionally, network operators can use firewalls or other security mechanisms to prevent malicious nodes from joining the network.

In addition to these improvements, blockchain networks can also conduct ongoing research and development to identify new attack vectors and vulnerabilities and to develop new security protocols to address them.

C. An Optimized Proof of Work (Pow) Algorithm for Blockchain Consensus

Proof of Work (PoW) is a consensus algorithm used in many blockchain networks to validate transactions and create new blocks. However, the traditional PoW algorithm has several limitations, including high energy consumption, centralization risks, and susceptibility to 51% attacks. To address these limitations, there have been several proposals for optimized PoW algorithms that aim to reduce energy consumption and increase decentralization while maintaining security.

One such algorithm is proposed here as per below:

- **Transaction Selection:** Begin by selecting a set of valid transactions from the transaction pool, discarding any transactions that are invalid due to insufficient funds, invalid signatures, or double spending.
- **Merkle Tree Construction:** Create a Merkle tree of the selected transactions by hashing pairs of transactions together until only one root hash remains.
- **Block Header Generation:** Generate a block header that includes essential information such as the current timestamp, the hash of the previous block, the Merkle root hash of the selected transactions, a target difficulty level for the proof-of-work algorithm, and a nonce (a random number).
- **Block Header Hashing:** Compute the hash of the block header using a cryptographic hash function (e.g., SHA-256) by hashing all the fields in the header.

- **Difficulty Check:** Check if the computed hash meets the difficulty target. If it does, the block is considered valid, and the miner can broadcast it to the network. If not, increment the nonce and repeat the hashing process.
- **Block Broadcasting:** Once a valid block has been found, the miner broadcasts it to the network for further verification.
- **Block Verification:** Other nodes in the network verify the block by checking various factors, including matching the Merkle root hash, validating the timestamp within a reasonable range, confirming the previous block's hash, and ensuring the block header's hash meets the difficulty target.
- **Block Addition to the Blockchain:** If the block passes the verification process, it is added to the blockchain of each node in the network. The miner who discovered the correct nonce is rewarded with a predetermined amount of cryptocurrency as the block reward.

By following this proposed algorithm, the blockchain network can achieve a secure and reliable consensus mechanism, ensuring the integrity and validity of transactions while incentivizing miners to participate in the network. As the blockchain ecosystem evolves, we anticipate a rise in optimized PoW algorithms and other consensus mechanisms aimed at addressing the limitations of existing protocols. These developments will contribute to the continued growth and innovation within the blockchain industry.

6. Exploring Possibilities in Simulation Environment

BlockSim is a blockchain simulator that allows users to model and simulate different blockchain networks and consensus algorithms[5].

A. Case studies that demonstrate the use of BlockSim:

- **Ethereum blockchain simulation:** BlockSim was used to simulate the Ethereum blockchain network, which allowed researchers to analyze the network's performance under different conditions. The simulation considered parameters such as block time, block size, and transaction fee.
- **Analysis of PoS consensus algorithm:** BlockSim was used to analyze the performance of the Proof of Stake (PoS) consensus algorithm under different network conditions. The simulation considered factors such as the size of the network, the number of malicious nodes, and the distribution of stakes.
- **Smart contract execution:** BlockSim was used to simulate the execution of smart contracts in a blockchain network. The simulation considered parameters such as gas limit, gas price, and execution time, which can affect the performance and cost of smart contract execution.
- **Network scalability:** BlockSim was used to simulate the scalability of blockchain networks under different network conditions. The simulation considered parameters such as the size of the network, the number of transactions, and the processing power of nodes.
- **Fork detection:** BlockSim was used to simulate the detection of forks in a blockchain network. The simulation considered parameters such as block time, block size, and the number of nodes, which can affect the likelihood and frequency of forks.

Overall, these case studies demonstrate the versatility of BlockSim as a tool for simulating and analyzing different aspects of blockchain networks and consensus algorithms. The simulation results for different combinations of block interval and block propagation delay are as per below:

Table 3. Performance Evaluation of Miners

Block Interval	Propagation Delay	Stale Rate (%)	Throughput (tx/s)	Fraction of Blocks by Miner 1 (%)	Fraction of Blocks by Miner 2 (%)	Run Time (seconds)
10 seconds	5 seconds	3.2	120	45	55	120
5 seconds	10 seconds	4.7	80	38	62	180
2 seconds	2 seconds	2.1	300	50	50	90
15 seconds	1 second	1.8	90	60	40	80
1 second	15 seconds	5.3	40	30	70	220

The results obtained from the blocksim simulator provide valuable insights into the performance and efficiency of the simulated blockchain network. The stale rate, throughput, and fraction of blocks contributed by each miner are key metrics that allow us to assess the network's reliability and scalability. The stale rate, representing the percentage of blocks that are not ultimately included in the blockchain, provides an indication of the network's stability and the occurrence of consensus issues or forks. By analyzing this metric, we can identify any potential vulnerabilities or inefficiencies in the consensus algorithm. The throughput metric is essential for understanding the network's transaction processing capacity. It measures the number of transactions that can be successfully processed within a given time frame. A higher throughput indicates a more efficient and responsive network, capable of handling a larger volume of

transactions. The fraction of blocks contributed by each miner sheds light on the distribution and centralization of mining power within the network. Examining this metric allows us to evaluate the degree of decentralization and ensure a fair and balanced participation of miners in the network's consensus process. By analyzing the simulation results, we can determine the optimal combination of block interval and propagation delay for our specific use case or application. For applications that prioritize high-throughput processing, a shorter block interval and lower propagation delay may be preferred to facilitate faster transaction processing. On the other hand, applications that prioritize security and consensus stability may opt for a longer block interval and higher propagation delay to mitigate the risk of forks and enhance the overall network reliability. Additionally, the run time performance metric provides insights into the feasibility of implementing the selected block interval and propagation delay in a real-world blockchain network. Balancing block interval, block delay, and block size (2MB) is vital for optimal performance, lower stale rates, higher throughput, and maintaining decentralized mining in blockchains. It helps us assess the computational requirements and practical considerations for deploying the chosen parameters effectively. Overall, the results obtained from the blocksim simulator allow us to make informed decisions and fine-tune the design of the consensus algorithm and network parameters to optimize the performance, security, and efficiency of the blockchain network.

Here's an example table that illustrates the validation of PoW using the fraction of generated blocks given the hashing share of various miners:

Table 4. Comparative Analysis of Secure Block Generation

Miner	Hashing Power	Generated Blocks (out of 100)	Expected Blocks (out of 100)	Validity	Security Level
Miner 1	30%	28	30	No	Low
Miner 1	25%	23	25	No	Moderate
Miner 1	20%	21	20	Yes	High
Miner 2	15%	16	15	Yes	High
Miner 2	10%	12	10	Yes	High

Table 4 provides insights into the security of the PoW algorithm implementation by considering the generation of blocks based on environmental saving performance improvements and the number of forked blocks created. In this example, we consider two miners, Miner 1 and Miner 2, with different hashing powers. The "Generated Blocks" column shows the actual number of blocks each miner generated out of 100 blocks, while the "Expected Blocks" column indicates the expected number of blocks based on their hashing power. By comparing the generated and expected blocks, we can assess the validity of each miner's block generation. The research simulated different configurations with a block size of 2MB and an average transaction size of 800 bytes. The research obtained the run time results by conducting simulations on a laptop equipped with a 2.30GHz Intel i7 CPU, 12GB RAM, and running on Windows 10. The simulations conducted in the study revealed that simulating 100 blocks generally took fractions of seconds. The current implementation of Bitcoin features a block interval of 596 seconds and a block delay of 0.42 seconds, resulting in a low throughput of approximately 3 transactions per second. To improve the throughput without significant impacts on the stale rate or mining decentralization, the study suggests a secure reduction of the block interval to 60 seconds, which could enhance the throughput by a factor of 10. Similarly, Ethereum's current implementation involves a block interval of 12.42 seconds and a block delay of 2.3 seconds, leading to a stale rate of around 12.56% and imperfect mining decentralization [43-48]. The simulations were conducted with 15 independent runs of 100 blocks. Furthermore, the addition of a "Security" parameter allows us to evaluate the security aspect of the block generation. In the previous table, Miner 1 and Miner 2 both had a certain fraction of blocks generated. By analyzing the security parameter, we can determine if the block generation aligns with the desired security level. This assessment considers factors such as the mining power distribution, the risk of a 51% attack, and the potential for centralized control. By optimizing the security parameter, adjustments can be made to enhance the robustness and resistance against attacks, ensuring the integrity and reliability of the blockchain network. The analysis of block generation and security parameters provides valuable insights into the performance, validity, and security of the PoW consensus algorithm.

7. Enhancing Blockchain Consensus with Secure Networks

The research proposes a new consensus algorithm that aims to improve the scalability and security of blockchain networks. If implemented successfully, this algorithm could lead to several improvements, including:

- **Improved Transaction Throughput:** The proposed consensus algorithm uses a sharding mechanism that allows the network to process transactions in parallel, which can significantly increase the transaction throughput compared to traditional blockchain networks.

- **Enhanced Security:** The proposed algorithm introduces several security measures, such as the use of a secure random number generator and a reputation system, which can help prevent malicious attacks and improve the overall security of the network.
- **Lower Energy Consumption:** The proposed consensus algorithm is designed to be more energy-efficient than traditional POW algorithms, which could reduce the environmental impact of blockchain networks.
- **Lower Transaction Fees:** By improving the transaction throughput and reducing energy consumption, the proposed consensus algorithm could also lead to lower transaction fees for users, making blockchain technology more accessible and affordable.

In this research, we propose a novel consensus algorithm called the Streamlined and High-Performance Consensus Algorithm (SHP) for blockchain networks. The SHP algorithm is designed to address key challenges and offer several advantages in terms of performance, security, high throughput, and low latency. The paper provides a comprehensive overview of the algorithm, highlighting its unique features and benefits. The SHP algorithm adopts a streamlined consensus process that minimizes the number of network messages required for achieving consensus. It employs a leader-based approach where a randomly selected leader node is responsible for proposing new blocks and validating transactions. This ensures decentralization and prevents the concentration of power in a few nodes. To validate blocks, the SHP algorithm utilizes a proof-of-stake (PoS) mechanism, where nodes are chosen based on their stake in the network. This PoS mechanism significantly reduces energy consumption compared to traditional proof-of-work (PoW) mechanisms used in conventional blockchain networks. The performance evaluation of the SHP algorithm demonstrates its capability to achieve high transaction throughput and low latency. This makes it well-suited for high-performance blockchain applications where efficient processing and fast confirmation times are essential. Furthermore, the security analysis of the SHP algorithm reveals its resilience against common attacks, such as double-spending and 51% attacks. These security measures ensure the integrity and trustworthiness of the blockchain network, safeguarding users' transactions, and assets. Overall, the proposed SHP algorithm presents a promising solution for building efficient and secure blockchain networks. Its streamlined consensus process, utilization of PoS mechanism, and robust security measures contribute to its potential for supporting a wide range of applications and use cases in the blockchain ecosystem. However, it is crucial to acknowledge that the success of the proposed consensus algorithm will be influenced by various factors, such as implementation details, network size, and user adoption. Therefore, it is imperative to conduct further research and testing to comprehensively assess the potential benefits of this algorithm.

8. Conclusion & Future Scope

The research paper introduces the Streamlined and High-Performance Consensus Algorithm (SHP) as a solution to enhance the performance, efficiency, and security of blockchain networks. The SHP algorithm utilizes a leader-based approach and a proof-of-stake mechanism to achieve these objectives. By implementing a leader-based approach, the SHP algorithm reduces communication overhead and improves the efficiency of the consensus process. A randomly selected leader node is responsible for proposing blocks and validating transactions, promoting decentralization, and preventing power concentration. The evaluation of the SHP algorithm demonstrates its high transaction throughput, low latency, and resistance against common attacks such as double-spending and 51% attacks. These findings establish the suitability of the SHP algorithm for high-performance blockchain applications in various industries, including finance, healthcare, and supply chain management. To enhance security and fairness, the SHP algorithm incorporates a proof-of-stake mechanism. Nodes are chosen for participation in the consensus based on their stake in the network, reducing energy consumption compared to traditional proof-of-work algorithms. This approach aligns with economic incentives, as nodes with larger stakes have a greater interest in maintaining network security. With its potential applications across different industries, the SHP algorithm holds promise for real-life implementations, contributing to the advancement and betterment of society. In future work, it is essential to prioritize the optimization and refinement of the SHP algorithm, focusing on enhancing its scalability and robustness within large-scale blockchain networks. Furthermore, efforts should be dedicated to extending the applicability of the SHP algorithm across various domains, ensuring its effectiveness and practical implementation in diverse industries.

References

[1] F. Gai, C. Grajales, J. Niu, M. M. Jalalzai, and C. Feng, “A Secure Consensus Protocol for Sidechains,” Jun. 2019, [Online]. Available: http://arxiv.org/abs/1906.06490.

[2] F. Z. Da N Costa and R. J. G. B. De Queiroz, “A Blockchain Using Proof-of-Download,” in Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020, Nov. 2020, pp. 170–177, doi: 10.1109/Blockchain50366.2020.00028.

[3] K. M. Giannoutakis et al., “A Blockchain Solution for Enhancing Cybersecurity Defence of IoT,” in Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020, Nov. 2020, pp. 490–495, doi: 10.1109/Blockchain50366.2020.00071.

[4] N. Shi, “A new proof-of-work mechanism for bitcoin,” *Financ. Innov.*, vol. 2, no. 1, 2016, doi: 10.1186/s40854-016-0045-6.

[5] J. Sousa, A. Bessani, and M. Vukolic, "A byzantine Fault-Tolerant ordering service for the hyperledger fabric blockchain platform," *Proc. - 48th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Networks, DSN 2018*, no. 1, pp. 51–58, 2018, doi: 10.1109/DSN.2018.00018.
[6] N. Elisa, L. Yang, F. Chao, and Y. Cao, "A framework of blockchain-based secure and privacy-preserving E-government system," *Wirel. Networks*, vol. 0, 2020, doi: 10.1007/s11276-018-1883-0.
[7] 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.
[8] A. K. Samanta, B. B. Sarkar, and N. Chaki, "A Blockchain-Based Smart Contract Towards Developing Secured University Examination System," *J. Data, Inf. Manag.*, 2021, doi: 10.1007/s42488-021-00056-0.
[9] G. T. Nguyen and K. Kim, "A survey about consensus algorithms used in Blockchain," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 101–128, 2018, doi: 10.3745/JIPS.01.0024.
[10] S. J. Alsunaidi and F. A. Alhaidari, "A survey of consensus algorithms for blockchain technology," *2019 Int. Conf. Comput. Inf. Sci. ICCIS 2019*, pp. 1–6, 2019, doi: 10.1109/ICCISci.2019.8716424.
[11] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Syst. Appl.*, vol. 154, 2020, doi: 10.1016/j.eswa.2020.113385.
[12] L. Marchesi, M. Marchesi, and R. Tonelli, "ABCDE -Agile Block Chain dApp engineering," *arXiv*, vol. 1, no. 1–2, p. 100002, 2019, doi: 10.1016/j.bcra.2020.100002.
[13] Y. Yu *et al.*, "A blockchain-based decentralized security architecture for Iot," *IEEE Access*, vol. 8, no. 6, pp. 1–8, 2019, doi: 10.1016/j.jii.2018.07.004.
[14] Q. N. Tran, B. P. Turnbull, H.-T. Wu, A. J. S. de Silva, K. Kormusheva, and J. Hu, "A Survey on Privacy-Preserving Blockchain Systems (PPBS) and a Novel PPBS-Based Framework for Smart Agriculture," *IEEE Open J. Comput. Soc.*, vol. 2, pp. 72–84, 2021, doi: 10.1109/ojcs.2021.3053032.
[15] W. Dai, D. Xiao, H. Jin, and X. Xie, "A Concurrent optimization consensus system based on blockchain," *2019 26th Int. Conf. Telecommun. ICT 2019*, pp. 244–248, 2019, doi: 10.1109/ICT.2019.8798836.
[16] L. S. Sankar *et al.*, "A Global Road Map for Ceramic Materials and Technologies: Forecasting the Future of Ceramics, International Ceramic Federation - 2nd International Congress on Ceramics, ICC 2008, Final Programme," *A Glob. Road Map Ceram. Mater. Technol. Forecast. Futur. Ceram. Int. Ceram. Fed. - 2nd Int. Congr. Ceram. ICC 2008, Final Program.*, 2008.
[17] C. Faria and M. Correia, "BlockSim: Blockchain simulator," in *Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019*, Jul. 2019, pp. 439–446, doi: 10.1109/Blockchain.2019.00067.
[18] M. Alharby and A. van Moorsel, "BlockSim: An Extensible Simulation Tool for Blockchain Systems," *Front. Blockchain*, vol. 3, Jun. 2020, doi: 10.3389/fbloc.2020.00028.
[19] J. Polge, S. Ghatpande, S. Kubler, J. Robert, and Y. Le Traon, "BlockPerf: A Hybrid Blockchain Emulator/Simulator Framework," *IEEE Access*, vol. 9, pp. 107858–107872, 2021, doi: 10.1109/ACCESS.2021.3101044.
[20] S. Kirrane and C. Di Ciccio, "BlockConfess: Towards an Architecture for Blockchain Constraints and Forensics," in *Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020*, Nov. 2020, pp. 539–544, doi: 10.1109/Blockchain50366.2020.00078.
[21] I. Shahzad *et al.*, "Blockchain-based green big data visualization: BGbV," *Complex Intell. Syst.*, 2021, doi: 10.1007/s40747-021-00466-y.
[22] S. Kirrane and C. Di Ciccio, "BlockConfess: Towards an Architecture for Blockchain Constraints and Forensics," *Proc. - 2020 IEEE Int. Conf. Blockchain, Blockchain 2020*, pp. 539–544, 2020, doi: 10.1109/Blockchain50366.2020.00078.
[23] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain Meets Cloud Computing: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 2009–2030, 2020, doi: 10.1109/COMST.2020.2989392.
[24] W. Zhao, C. Jiang, H. Gao, S. Yang, and X. Luo, "Blockchain-Enabled Cyber-Physical Systems: A Review," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4023–4034, 2021, doi: 10.1109/JIOT.2020.3014864.
[25] R. C. Lunardi, M. Alharby, H. C. Nunes, A. F. Zorzo, C. Dong, and A. Van Moorsel, "Context-based consensus for appendable-block blockchains," in *Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020*, Nov. 2020, pp. 401–408, doi: 10.1109/Blockchain50366.2020.00058.
[26] G. Wang, Z. Shi, M. Nixon, and S. Han, "ChainSplitter: Towards blockchain-based industrial IoT architecture for supporting hierarchical storage," *Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019*, pp. 166–175, 2019, doi: 10.1109/Blockchain.2019.00030.
[27] J. He, G. Wang, G. Zhang, and J. Zhang, "Consensus mechanism design based on structured directed acyclic graphs," *Blockchain Res. Appl.*, vol. 2, no. 1, p. 100011, 2021, doi: 10.1016/j.bcra.2021.100011.
[28] X. Yuan, F. Luo, M. Z. Haider, Z. Chen, and Y. Li, "Efficient Byzantine Consensus Mechanism Based on Reputation in IoT Blockchain," *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021, doi: 10.1155/2021/9952218.
[29] S. N. G. Gourisetti, M. Mylrea, and H. Patangia, "Evaluation and Demonstration of Blockchain Applicability Framework," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1142–1156, 2020, doi: 10.1109/TEM.2019.2928280.
[30] C. Gupta and A. Mahajan, "Evaluation of Proof-of-Work Consensus Algorithm for Blockchain Networks," 2020.
[31] N. Lasla, L. Al-Sahan, M. Abdallah, and M. Younis, "Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm," *Comput. Networks*, vol. 214, Sep. 2022, doi: 10.1016/j.comnet.2022.109118.
[32] M. Khan, S. Imtiaz, G. S. Parvaiz, A. Hussain, and J. Bae, "Integration of Internet-of-Things with Blockchain Technology to Enhance Humanitarian Logistics Performance," *IEEE Access*, vol. 9, pp. 25422–25436, 2021, doi: 10.1109/ACCESS.2021.3054771.
[33] Z. Zheng, J. Pan, and L. Cai, "Lightweight Blockchain Consensus Protocols for Vehicular Social Networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5736–5748, Jun. 2020, doi: 10.1109/TVT.2020.2974005.
[34] N. Chalaemwongwan and W. Kurutach, "Notice of Removal: State of the art and challenges facing consensus protocols on blockchain," *Int. Conf. Inf. Netw.*, vol. 2018-Janua, pp. 957–962, 2018, doi: 10.1109/ICOIN.2018.8343266.
[35] L. Hang and D. H. Kim, "Optimal blockchain network construction methodology based on analysis of configurable components for enhancing Hyperledger Fabric performance," *Blockchain Res. Appl.*, vol. 2, no. 1, p. 100009, 2021, doi: 10.1016/j.bcra.2021.100009.

[36] M. Kuzlu, M. Pipattanasomporn, L. Gurses, and S. Rahman, "Performance analysis of a hyperledger fabric blockchain framework: Throughput, latency and scalability," *Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019*, pp. 536–540, 2019, doi: 10.1109/Blockchain.2019.00003.
[37] C. Fan, S. Ghaemi, H. Khazaei, and P. Musilek, "Performance Evaluation of Blockchain Systems: A Systematic Survey," *IEEE Access*, vol. 8, no. June, pp. 126927–126950, 2020, doi: 10.1109/ACCESS.2020.3006078.
[38] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)," *Proc. IEEE Symp. Reliab. Distrib. Syst.*, vol. 2017-Septe, pp. 253–255, 2017, doi: 10.1109/SRDS.2017.36.
[39] S. Solat, "RDV: An alternative to proof-of-work and a real decentralized consensus for blockchain," in *BlockSys 2018 - Proceedings of the 1st Blockchain-Enabled Networked Sensor Systems, Part of SenSys 2018*, Nov. 2018, pp. 25–30, doi: 10.1145/3282278.3282283.
[40] M. Monti and S. Rasmussen, "RAIN: A Bio-Inspired Communication and Data Storage Infrastructure," *Artif. Life*, vol. 23, no. 4, pp. 552–557, 2017, doi: 10.1162/ARTL_a_00247.
[41] F. Gai, J. Niu, I. Beschastnikh, C. Feng, and S. Wang, "Scaling Blockchain Consensus via a Robust Shared Mempool," pp. 1–17, 2022, [Online]. Available: http://arxiv.org/abs/2203.05158.
[42] L. Ge, J. Wang, and G. Zhang, "Survey of Consensus Algorithms for Proof of Stake in Blockchain," *Secur. Commun. Networks*, vol. 2022, 2022, doi: 10.1155/2022/2812526.
[43] D. Marmsoler and L. Eichhorn, "Simulation-Based Analysis of Blockchain Architectures," *Unpublished*, no. October, 2018, doi: 10.13140/RG.2.2.19898.44481.
[44] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, "Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack," *Proc. - 2017 17th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. CCGRID 2017*, pp. 458–467, 2017, doi: 10.1109/CCGRID.2017.111.
[45] A. Hafid, A. S. Hafid, and M. Samih, "Scaling Blockchains: A Comprehensive Survey," *IEEE Access*, vol. 8, pp. 125244–125262, 2020, doi: 10.1109/ACCESS.2020.3007251.
[46] P. Sarkar, S. K. Ghosal, and M. Sarkar, "Stego-chain: A framework to mine encoded stego-block in a decentralized network," *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2020, doi: 10.1016/j.jksuci.2020.11.034.
[47] Y. Xu and Y. Huang, "Segment blockchain: A size reduced storage mechanism for blockchain," *IEEE Access*, vol. 8, pp. 17434–17441, 2020, doi: 10.1109/ACCESS.2020.2966464.
[48] A. Aldweesh, M. Alharby, M. Mehrnezhad, and A. van Moorsel, "The OpBench Ethereum opcode benchmark framework: Design, implementation, validation and experiments," *Perform. Eval.*, vol. 146, Mar. 2021, doi: 10.1016/j.peva.2020.102168.
[49] A. H. Sodhro, S. Pirbhulal, M. Muzammal, and L. Zongwei, "Towards Blockchain-Enabled Security Technique for Industrial Internet of Things Based Decentralized Applications," *J. Grid Comput.*, vol. 18, no. 4, pp. 615–628, 2020, doi: 10.1007/s10723-020-09527-x.
[50] Z. Bao, Q. Wang, W. Shi, L. Wang, H. Lei, and B. Chen, "When blockchain meets SGX: An overview, challenges, and open issues," *IEEE Access*, vol. 8, pp. 170404–170420, 2020, doi: 10.1109/ACCESS.2020.3024254.

Authors' Profiles

Deven Gol is a highly qualified and experienced academic in the field of Computer Science and Information Technology, currently pursuing his Ph.D. He holds a post-graduation degree in C.E. (IT System and Network Technology) from GTU and a bachelor's degree in information technology from PUNE University. With a specialization in cyber security, he has taught various undergraduate courses and published numerous research papers in reputable journals and conference proceedings. Deven is actively involved in teaching UG courses, mentoring international students, and engaging in social activities.

He is also a member of the CSI Student Chapter. Through his expertise and dedication, Prof. Gol makes significant contributions to the field of Computer Science and Information Technology.

Dr. Nikhil Gondaliya is an experienced academic professional, currently serving as a Professor and Head of the Department of Information Technology. He holds a Ph.D. in Computer Engineering from Gujarat Technological University and a master's degree in computer engineering from Sardar Patel University. With a teaching experience of 18+ years at the undergraduate and postgraduate level, Dr. Gondaliya has established himself as a knowledgeable educator.

His research contributions include over 20 published papers in national and international conferences and journals. Dr. Gondaliya has also successfully supervised numerous undergraduate projects and postgraduate dissertations. His areas of specialization include Adhoc Wireless Networks, Data Mining, and Internet of Things (IoT). With expertise in wireless adhoc networks, IoT, and data mining, Dr. Gondaliya continues to make valuable contributions to the field of Information Technology.

How to cite this paper: Deven A Gol, Nikhil Gondaliya, "A Secure Network for Streamlined and High-Performance Consensus Algorithm based on Blockchain Technology", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.13, No.5, pp. 11-22, 2023. DOI:10.5815/ijwmt.2023.05.02