Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 11, Issue 3, pp: (41-56), Month: September - December 2024, Available at: www.noveltyjournals.com

Design and Analysis of Efficient Consensus Algorithms to Enhance the Security and Performance of Blockchain

Anjaneyulu Endurthi[1], Akhil Khare[2]

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

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

DOI: https://doi.org/10.5281/zenodo.14012653

Published Date: 30-October-2024

Abstract: **Blockchain is a transformative technology that enables secure, transparent, and decentralized digital transactions by storing data across a distributed network of computers. It eliminates the need for intermediaries by using cryptographic techniques to ensure the integrity and immutability of records. Blockchain is revolutionizing various industries, from finance to supply chain management. Consensus algorithms are the foundational protocols in blockchain networks that ensure all participating nodes agree on the validity of transactions, maintaining the system's security and consistency without central authority. Two consensus algorithms were proposed which are based on proof of work and proof of stake. The first one is a two-phase consensus algorithm, The first phase consists of proof of stake and the second stage consists of proof work. The Second proposed algorithm is based on the coin-age selection criteria of proof of stake. The proposed algorithms were simulated and analyzed for their security and performance with the existing algorithms and published results. The proposed algorithms are far better in terms of performance and security as per the results achieved.**

Keywords: **Blockchain, Consensus Algorithms, Coin-age Selection, Proof of Work, Proof of Stake, Performance, Security.**

1. INTRODUCTION

Blockchain technology can potentially transform society by enabling decentralised, transparent, and secure transactions without the need for intermediaries. Its initial prominence came from its association with cryptocurrencies like Bitcoin. Blockchain is poised to significantly transform various aspects of our lives, including how we interact and conduct business. Recently, the academic, industrial, and research communities are doing research on blockchain, to make it more convenient and accessible across various sectors.

The idea of a secure chain of blocks dates back to the early 90's. It was introduced by Stuart Haber [1] and colleagues in the year 1991 as a method for digitally timestamping the data which is present in the form of electronic documents to prevent tampering. However, the blockchain has gained widespread recognition only when Blockchain technology was employed to record transactions of the cryptocurrency ''Bitcoin'' [2].

1.1 Blockchain background

The following background is required for understanding Blockchain

1.1.1 Peer-To-Peer (P2p) Network

A P2P network is a decentralized [3] structure in which players collectively share resources. Every member (peer) in this network has the ability to function as both a client and a server. For instance, Peer A, in the role of a client, can directly solicit services or material from Peer B, in the role of a server, without the necessity of intermediaries. Subsequently, Peer A has the potential to function as a server, receiving requests from Peer B while simultaneously functioning as a client.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 11, Issue 3, pp: (41-56), Month: September - December 2024, Available at: www.noveltyjournals.com

1.1.2 Cryptography

It is the field of mathematics that focuses on ensuring the security of communication. It has a crucial role in contemporary security protocols. A 'key' is an essential mathematical value in the field of cryptography. Modern cryptography can be categorized into two distinct types: Symmetric key cryptography involves the utilization of a single key for cryptographic operations by both the sender and the receiver. Asymmetric key cryptography involves the use of two separate keys by each party: a public key and a private key. These keys are utilized for different cryptographic processes. Cryptography encompasses a range of procedures aimed at offering security services, including confidentiality (maintaining the privacy of information), integrity (ensuring data remains unchanged), authentication (verifying the identity of the sender) [4] [5] [6].

1.1.3 Merkle Tree

Merkle trees, commonly referred to as hash trees, effectively and securely validate data by arranging it and its related hash values into a hierarchical structure. Within this arrangement, every terminal node is assigned a hash value corresponding to specific data, while intermediary nodes store the hashes of their subordinate children. Merkle trees are essential for the proper functioning of Blockchain. Figure 1 depicts a Merkle tree [7].

1.1.4 Digital Signatures & Timestamp

Digital signatures are widely recognized as being genuine, impossible to counterfeit, and legally binding. Timestamping is the process of recording the precise date and time of an event, which allows for accurate comparison of information throughout different periods of time.

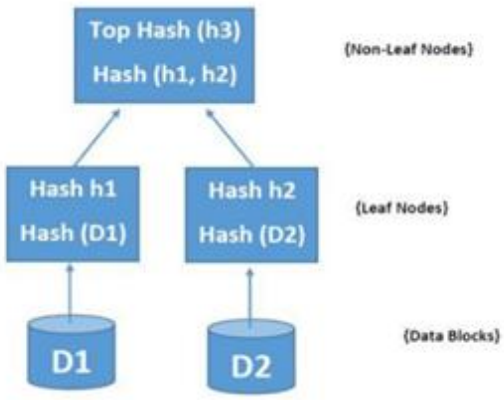

Figure 1. Merkle tree (Binary hash tree)

The following are key characteristics of Blockchain

1.1.5 Decentralization

The very inherent feature of blockchain is decentralization. The Blockchain ledger is decentralized and replicated across numerous computers (nodes) inside a network [8], [9], [10] and [11].

1.1.6 Transparency

Transactions recorded on the Blockchain ledger are fully transparent, enabling anybody to access transaction details and history. The exceptional level of openness exhibited by Blockchain technology guarantees the accountability and integrity of the information, effectively preventing any unauthorized modifications.

1.1.7 Security

Blockchain systems has intrinsic security features by utilizing asymmetric cryptography. This entails a collection of public keys that are accessible to all individuals and private keys that are exclusively available to the owner. These keys guarantee the ownership of transactions and prohibit any unauthorized alteration [12].

1.1.8 Immutability

Immutability, also referred to as un-tamperability, refers to the characteristic of the Blockchain where data, once added, becomes unchangeable and resistant to tampering. In a Blockchain, data blocks are marked with a timestamp and protected with hash algorithms, ensuring that the data remains unchanged and secure unless a consensus is established by the majority of nodes.

1.1.9 Traceability

Blockchain technology facilitates data traceability by monitoring the origin, destination, and order of data modifications among nodes. When information is uploaded or altered in a Blockchain, it is assigned a timestamp, which creates a transparent record of all the changes made.

1.1.10 Anonymity

Blockchain ensures privacy through anonymity, which involves authenticating transactions without revealing personal information about the involved parties.

1.1.11 Democracy

Within a Blockchain system, decisions are reached through a democratic process including all nodes, utilizing a peer-to-peer methodology. Consensus techniques are employed to ascertain which nodes have the authority to incorporate new blocks into the Blockchain and to guarantee the accurate appending and synchronization of the block across all nodes.

1.1.12 Integrity

Blockchain systems are intrinsically engineered to be impervious to changes in data, guaranteeing the preservation of data integrity over its entire lifespan. This implies that the transactions/data stored in the Blockchain remains precise and unchanging from the time it is initially recorded until it is no longer in existence.

1.1.13 Programmability

Blockchain technology is based on open source code, which enables users to create applications using a shared application programming interface (API). The versatile programming environment can be employed to generate intricate smart contracts or other decentralized applications.

1.1.14 Fault Tolerance

Blockchain systems are deliberately engineered to be redundant so as to ensure a high degree of immutability and fault tolerance [13]. Because of its p2p [14] design, it offers the network a significant level of tolerance, enabling it to remain operational even in the event of certain nodes becoming disconnected or experiencing network transit problems [15].

1.2 Performance Metrics

A metric is a benchmark used to quantify and evaluate performance. For example, the velocity and promptness can provide us with insights into the quality of a machine. Speed and responsiveness are key measures that provide insights into the performance and capabilities of a system, including its computational power, memory usage, and network behavior. When evaluating consensus methods, important metrics to be considered are throughput, time to reach consensus, and energy consumption. Performance metrics in distributed systems can be employed to quantify performance at several levels. The levels specified in references [16] are:

i. At the system level, performance can be monitored at its maximum level. It pertains to the overall functioning of the system and can be somewhat intricate to quantify.

ii. Service level: This pertains to the components performance collaborating as a group or deliver a particular service. The term used to refer to this concept is "distribution-unit cluster level".

iii. At the machine level, the evaluation focuses on measuring the performance of a single node.

iv. Process level: This level involves measuring the performance of an individual process.

Nevertheless, given that the majority of consensus rounds culminate in block production, which is then propagated to all nodes, the consequences can be observed at the system level. Hence system level metrics have been considered in this research in order to check the performance.

The consensus algorithms which are designed need to be compared against the following performance metrics.

i. Average Block Size
ii. Average Confirmation Time
iii. Average Difficulty
iv. Average Network Hash Rate
v. Network Utilization
vi. Average Transaction Fee
vii. Total Orphaned Blocks/Uncles
viii. Write Throughput
ix. Write Latency
x. Success Rate
xi. Security against attacks

Security Metrics

i. 51 % Attack
ii. Unfair Miner Selection
iii. Forking Issue
iv. Double Spending Problem
v. Rich Getting Richer Syndrome
vi. Validator Waiting Time
vii. Energy consumption
viii. Randomization of Validators
ix. True Decentralization

2. LITERATUR REVIEW

The consensus algorithm, a crucial element of the blockchain network, guarantees unanimous “agreement among all nodes in the network”. It eliminates the participation of centralized authority in verifying transactions. It guarantees that the majority of nodes reach a consensus on the present state of the ledger. Universal participation in the consensus process should be ensured, provided that the technique used is fair and equitable. Some consensus algorithms from the literature along with their merits and demerits have been discussed below.

2.1 Proof of Work

Proof of work is the first generally recognized concept in the world of blockchain technology, having been developed by Nakamoto. A number of cryptocurrencies use it as their consensus mechanism, including Bitcoin and Ethereum 1.0 [16]. Proof of Work, or PoW, is a process in which miners use expensive, specialized computers with GPUs to solve complex mathematical puzzles. Using trial and error approaches is the only practical way to solve riddles.

Advantages:

- PoW, or Proof Work, was the pioneering consensus protocol and has gained significant popularity. It has a high level of scalability, which makes it appropriate for a wide variety of applications.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 11, Issue 3, pp: (41-56), Month: September - December 2024, Available at: www.noveltyjournals.com

Drawbacks:

- This requires a significant amount of energy. The process is expensive and demands a substantial number of computational resources.
- It is susceptible to the well-known 51% attack, where a group of hostile miners controlling 51% of the network might seize control and establish supremacy, resulting in the failure of decentralization

2.2 Proof of Stake:

PoS [17], [18], [19], [20]. Blockchain networks are made more efficient by the consensus algorithm, which does away with the proof of work protocols' energy-consuming computational mining procedure. Under the proof of stake principle, a person or node can mine or validate a block of transactions based on how many coins or cryptocurrencies they own. As collateral, users must deposit their cash in order to become network validators. Similar to miners in proof-of-work, validators in proof-of-stake are in charge of organizing transactions and creating new blocks. This ensures that every node is in agreement with the network's current status and the freshly created block. Ethereum [21] and other alternative cryptocurrency versions employ the proof of stake concept.

Advantages:

- Increased velocity - Transactions are processed more quickly in comparison to PoW.
- Reduced energy use due to the absence of supercomputers.

Drawbacks:

- It remains susceptible to vulnerabilities. An individual with substantial financial resources has the ability to acquire a significant quantity of coins, which consequently diminishes the decentralization of the system.
- The phenomenon of wealth accumulation among the already affluent. Only individuals with significant wealth possess the ability to exert influence over the consensus.
- Problem of simulating at no cost

Verification and validation are done through the various methods [22], [23].

2.3 Delegated Proof of Stake (DPoS)

In a way similar to democracy, DPoS [24] selects delegates, who are in charge of confirming the next block through voting by network users. Block construction is the responsibility of the chosen delegates, who verifies transactions. The elected delegates receive this compensation in terms of reward after creating the block and adding it to the existing blockchain. The portion of the block reward increases as the stake is increased. The distribution of benefits and rewards depends on the investment made by each user.

Advantages:

- DPoS provides all the advantages of PoS. In addition to that, below are the other advantages:
- Improved allocation of prizes - Individuals solely select delegates based on the benefits they provide. This implies that individuals of all economic backgrounds are able to earn, rather than solely those who are wealthy. Therefore, DPoS exhibits a higher degree of decentralization compared to both PoS and PoW.
- Secure Real-time Voting — Users have the ability to promptly cast their votes to remove any delegate engaged in malicious activities.

Drawbacks:

- Cartel Formation - There is a possibility that witnesses may collaborate and establish cartels to govern the network.
- Vulnerability - Due to the limited number of individuals responsible for network maintenance, the likelihood of a 51% attack is increased.
- Centralized - Power is concentrated within a small group of individuals.

TABLE: 1 Consensus Protocols and Their Issues

Consensus protocols	Available issues
Proof of Work	Energy consumption, forking, 51% attack, unfair selection of miner
Proof of Stake	51% attack, forking, unfair selection of miner
Delegated Proof of Stake	51% attack, unfair selection of miner
Proof of Adjourn	Energy consumption, Unfair selection of transactions
Proof of Activity	Energy consumption, unfair selection of miner

3. PROPOSED METHOD I

The primary aim of this research is to develop a mining selection procedure that provides equal possibilities to all nodes in the network, while also assuring that each chosen miner runs with integrity. In this particular context, integrity refers to the act of exclusively incorporating legitimate transactions into the blockchain. In order to motivate miners to behave with integrity, it is necessary to have a stake at risk.

The proposed approach [25] is a hybrid paradigm that integrates both Proof of Stake and Proof of Work mechanisms. Proof of Stake is employed first, followed by Proof of Work. Within the initial tier, every node commits a specific quantity of currency and employs a selection approach known as the lowest unique integer bid strategy. This strategy determines which nodes, depending on their staked amount, will progress to the subsequent level of the algorithm, with only 10% of the nodes being selected.

The quantity of stake guarantees the honest operation of nodes. In the event that any unauthorized action is identified during the verification process, the node is required to surrender the cash it has staked. Hence, a minimum investment is necessary in order to prevent the occurrence of the "nothing-at-stake" dilemma. Furthermore, in order to be chosen as miners, nodes are need to carry out certain tasks. Nevertheless, if every node were to engage in mining, it would result in an exorbitant consumption of energy. In order to address this issue, only a mere 10% of the overall nodes are elevated to the subsequent stage of the algorithm (Proof of Work), resulting in a significant 90% reduction in energy consumption.

The selection approach utilizes the lowest unique integer bid, and this procedure is iterated multiple times to choose 10% of the nodes. These nodes have placed a minimal and distinctive stake, unparalleled by any others. This concept bears resemblance to a lottery system, where the miner is selected in a random manner. The selection process in this situation is entirely arbitrary, necessitating minimal expertise. The probability of winning is determined by two factors: firstly, the absence of any other player selecting the same number; and secondly, the smallest number of lower integers that have already been successful. Each participating node autonomously determines its optimal option by making predictions about the behaviors of other nodes, in accordance with the concept of Nash equilibrium. The suggested solution is depicted in the flowchart presented in Figure 2.

Our proposed technique guarantees equal and fair opportunity for all participating nodes by implementing a strategy similar to a lottery, where winning is determined by chance, using the lowest unique number. The risk of a 51% attack is completely eliminated by randomly selecting the miner, which requires minimal effort to become one. In this non-cooperative technique, nodes are inclined to place bids that are significantly higher than the lower value, as the likelihood of success diminishes with increasing bid amounts. Likewise, greater numbers are deliberately avoided since the likelihood of winning is nonexistent at those amounts. As a result, the blockchain is protected by a stake, which enhances the security of the blockchain.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 11, Issue 3, pp: (41-56), Month: September - December 2024, Available at: www.noveltyjournals.com

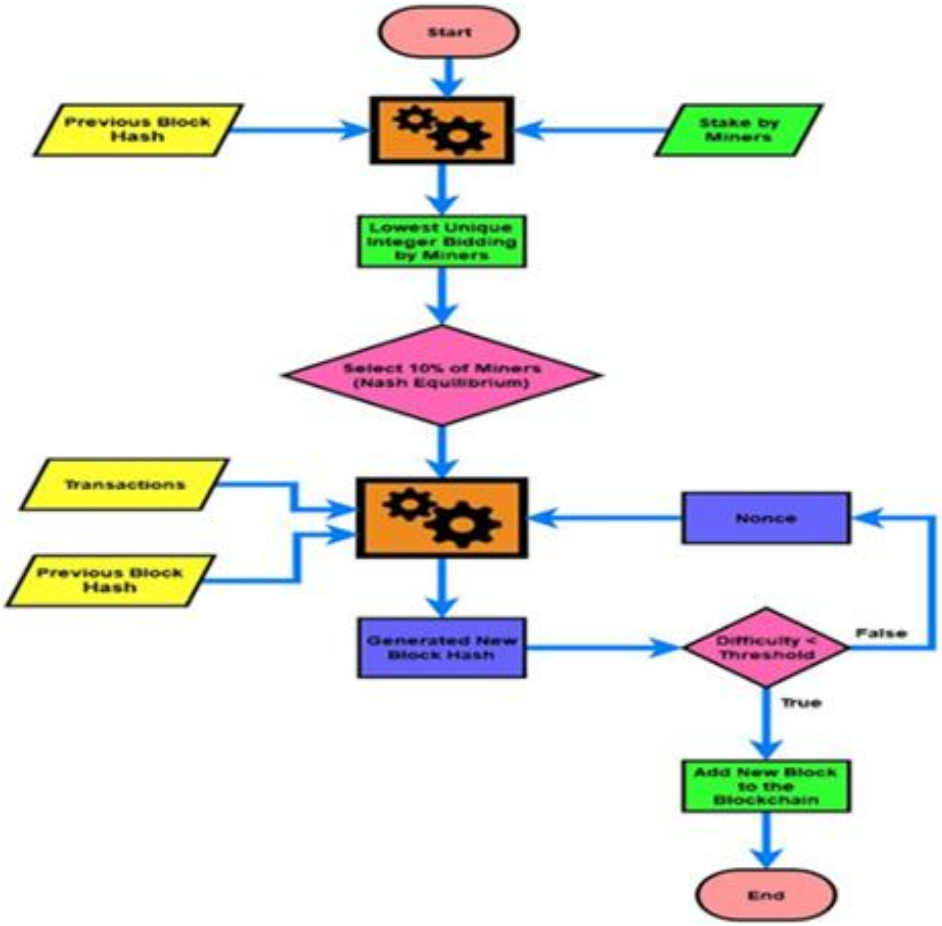

Figure 2: Proposed Algorithm Flowchart

4. PROPOSED METHOD II

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

In traditional approaches, native tokens [26] are staked directly for participation in validator elections. However, in the proposed method, the nodes that are interested in becoming validators should mint staking tokens derived from the native tokens. The timestamp of these staked tokens is used as a critical parameter to calculate the hash power of the peers.

The procedure for the same is given below:

1. A node seeking validator status initiates the creation of new tokens.

2. The newly created tokens are staked by the participants if they are interested in becoming the validator.

3. Each validator's hash power is computed using the method outlined in the subsequent section.

4. The hash power is used as a parameter to build the pie chart, facilitating visualization of the probabilities.

5. This pie chart is akin to a roulette wheel which is spun around randomly to select a validator. Thus, those with greater hash power possess higher probabilities of being elected as the validator to mine the next block.

6. After creating the new block, the tokens that were staked earlier are redistributed to all participating peers. Timestamps are applied based on whether the node emerged victorious or not.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 11, Issue 3, pp: (41-56), Month: September - December 2024, Available at: www.noveltyjournals.com

5. ANALYSIS OF PROPOSED CONSENSUS ALGORITHMS

This section discusses about the analysis of proposed algorithms against the most popular consensus algorithms – Proof of Work (PoW) and Proof of Stake (PoS).

To do the analysis, the following methods can be adopted:

i. Blockchain Explorers: Tools like Etherscan (for Ethereum), Blockchain.com (for Bitcoin), and others provide real-time data on transactions, blocks, fees, and more.

ii. Monitoring Tools: Tools like Prometheus and Grafana can be used to monitor blockchain nodes and network metrics in real-time.

iii. Benchmarking: Conduct tests by simulating different transaction loads and analyzing the impact on TPS, latency, and other metrics.

iv. Statistical Analysis: Utilize statistical techniques to examine past data, spot trends, and make predictions about future performance.

As part this research, the analysis is being carried out by collecting the data from the Blockchain explorers like Bitcoin blockchain for analyzing proof of work, Ethereum blockchain for analyzing proof of stake. The proposed algorithm I (as discussed in section 3) is analyzed by using the statistical methods and the Proposed algorithm II (as discussed in section 4) is analyzed by the benchmarking tools.

The consensus algorithms were compared against the following primary metrics and Secondary Metrics:

i. Average Block Size

ii. Average Confirmation Time

iii. Average Difficulty

iv. Average Network Hash Rate

v. Network Utilization

vi. Average Transaction Fee

vii. Total Orphaned Blocks/Uncles

viii. Write Throughput

ix. Write Latency

x. Success Rate

xi. Security against attacks

5.1 Average Block Size

The "average block size" refers to the mean size of blocks over a specific period of time on a blockchain, typically measured in kilobytes (KB) or megabytes (MB). It represents the average amount of data that is stored in each block, including transactions, smart contracts, and other relevant data.

Block size significantly impacts the performance of a blockchain in various ways. The data has been collected and analyzed for calculating the average size of the blocks and the average block size can be calculated by using the available data. Average Block size for the PoW comes to be around 1.5MB and that of PoS comes to be around 1MB. It is important to note that in the case of PoS, a block can only a maximum of 12MB in size.

In case of the proposed algorithm I, we have considered implementing an adaptive block size that can adjust based on network conditions. For example, during periods of low demand, the block size could shrink to save energy, while it could expand during high demand to handle more transactions. As a starting point, we might choose a block size that balances transaction throughput and network stability.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 11, Issue 3, pp: (41-56), Month: September - December 2024, Available at: www.noveltyjournals.com

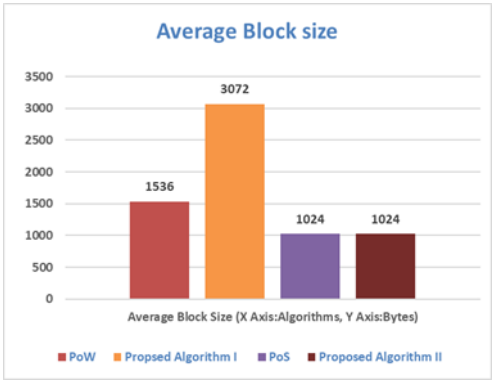

Figure 3: Comparison of Average Block size

5.2 Average Block Confirmation Time

It is the average amount of time that passes after a transaction is broadcast to the network until a block is validated and put to the blockchain. This time is a crucial measure for blockchain technology since it affects the network's overall speed and effectiveness.

A similar procedure has been followed to calculate the average block confirmation time in case of PoW and PoS.

The average block confirmation time for PoW comes to be 8848.160393 seconds and for PoS it comes to be around 14.00585277 seconds.

Estimating the Combined Confirmation Time:

The total block confirmation time for the proposed algorithm I, will depend on how much time each phase takes and how they interact. Since PoW is significantly longer, it will dominate the confirmation time. Let's estimate the confirmation time as a weighted sum of the PoS and PoW phases:

TProposed I=TPoS+TPoW

Estimation:

PoS Phase: TPoS≈14 seconds

PoW Phase: TPoW≈8848 seconds

Thus,

TProposed I≈14 seconds+8848 seconds≈8862 seconds.

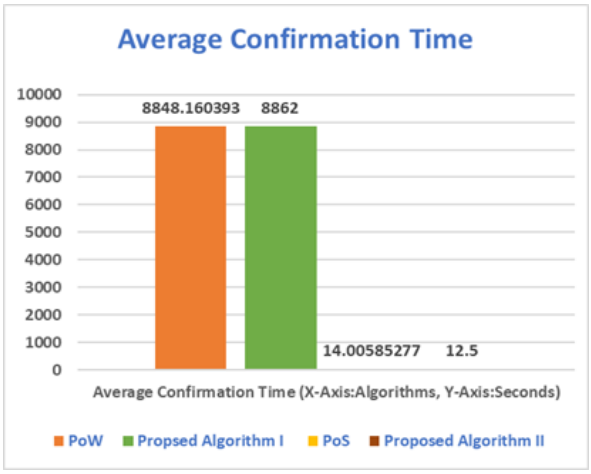

Figure 4: Comparison of Average confirmation Time

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 11, Issue 3, pp: (41-56), Month: September - December 2024, Available at: www.noveltyjournals.com

5.3 Average Difficulty

Average difficulty refers to the mean level of difficulty over a specific period that miners or validators must overcome to successfully add a created block to the existing chain. It is a gauge of how difficult it is to verify a block by determining the proper hash (in Proof of Work) or by meeting other requirements (in Proof of Stake or other consensus techniques).

The average difficulty of creating a block in case of PoW is 11781764142115.50 and PoS is 2865.364813

The average difficulty of the proposed algorithm I would likely fall between the difficulties of the traditional PoW and PoS system. The difficulty can be considered as a weighted average of the difficulties of the PoW and PoS phases.

Given:

PoW Difficulty: 11,781,764,142,115.50 TH

PoS Difficulty: 2,865.364813 TH

Estimating the Average Difficulty for the proposed algorithm I:

we could use a simple average:

Average Difficulty=PoW Difficulty+PoS Difficulty/2

Average Difficulty=11,781,764,142,115.50+2,865.364813/2

Average Difficulty=5,890,882,072,490.432407

The estimated average difficulty for the proposed algorithm I, assuming equal weighting of PoW and PoS phases, would be approximately 5,890,882,072,490.43 TH

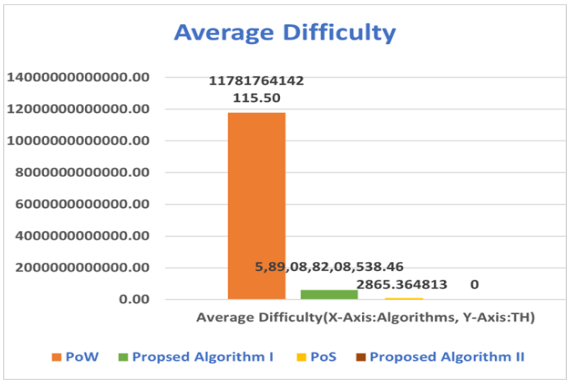

Figure 5: Comparison of Average Difficulty

5.4 Average Network Hash Rate

Network Hash Rate refers to the total computational power that is being used by all miners on a blockchain network, particularly those using a Proof of Work (PoW) consensus algorithm. It is a measure of how many hash operations (calculations) are being performed per second across the entire network to find the correct hash for the next block.

Similarly, the network has rate can be calculated for the proposed algorithm I by using the PoS & PoW network hash rates which are is 85722488.2257691 Million Tera hashes/sec for the PoW and the PoS network hash rate is 220698.486674977 Giga hashes/sec. To calculate the network hash rate of the proposed algorithm I, we need to consider the network hash rates of both the Proof of Work (PoW) and Proof of Stake (PoS) components, as well as the fact that only 10% of nodes are involved in the PoW phase.

Given:

PoW Network Hash Rate: 85,722,488.2257691 Million Tera hashes/sec

PoS Network Hash Rate: 220,698.486674977 Giga hashes/sec

Converting Units to a Common Base:

PoW Hash Rate=85,722,488.2257691 Million Tera hashes/sec

=85,722,488.2257691×106 TH/Sec

=85,722,488.2257691×1012 Giga hashes/sec

PoS Hash Rate=220,698.486674977 Giga hashes/sec

Average Network hash rate of the proposed algorithm I:

Since only 10% of the nodes participate in the PoW phase:

Adjusted PoW Hash Rate=85,722,488.2257691×1012/10

Adjusted PoW Hash Rate=8,572,248.82257691×1012 Giga hashes/sec

Combining PoW and PoS Hash Rates:

Total Hash Rate=Adjusted PoW Hash Rate+PoS Hash Rate

Total Hash Rate≈8,572,249.043275396×1012 Giga hashes/sec

The estimated network hash rate for the proposed algorithm I would be approximately 8,572,249.043275396 Tera hashes/sec (or 8.572 Million Peta hashes/sec= 8,572,249.043 Million Tera hashes/sec.).

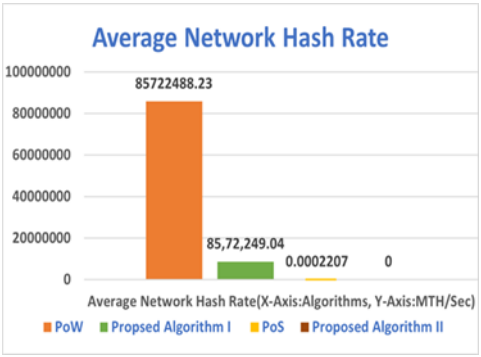

Figure 6: Comparison of Average Network Hash Rate

5.5 Network Utilization

Network utilization generally refers to how effectively the computational resources (hash rate) of the decentralized network are being used to secure the blockchain and process transactions.

It can be represented as:

Network Utilization=Effective Hash Rate / Total Hash Rate

Where, Effective Hash Rate is the portion of the hash rate that is actually contributing to block production and Total Hash Rate is the overall hash rate of the network. By using the statistical data, the network utilization of PoW is 78% and PoS is 57.55%.

Given: PoW Network Utilization: 78%

PoS Network Utilization: 57.55%

Participation Rate in PoW Phase: 10%

Participation Rate in PoS Phase: 90%

The network utilization for the proposed algorithm I can be calculated using the following formula:

Network Utilization = (0.1×PoW Utilization)+(0.9×PoS Utilization)

The estimated network utilization of the proposed algorithm I is 59.595%.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 11, Issue 3, pp: (41-56), Month: September - December 2024, Available at: www.noveltyjournals.com

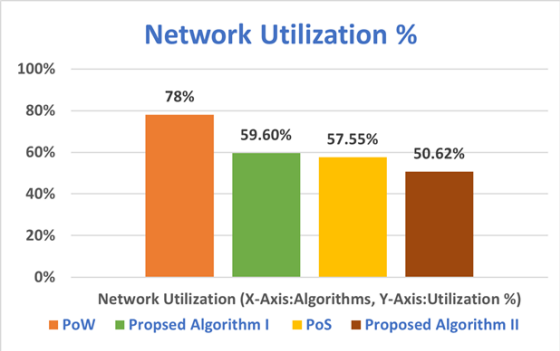

Figure 7: Comparison of Network Utilization

5.6 Write Throughput

Write throughput usually refers how many transactions or how much data is being successfully recorded on the blockchain per unit of time. It can be measured in transactions per second (TPS) or data per second.

The write throughput of PoW:

Total number of transactions recorded on blockchain till now= 1.057 Billion Transactions

Total time =92566400 Seconds

Thus write throughput = 1.057 Billion Transactions/92566400 Seconds

= 2.145903578

Similarly write throughput of PoS is 1100.400841558

Write throughput of the proposed algorithm I:

Weighted Average Calculation:

Write Throughput = (0.1×PoW Throughput) + (0.9×PoS Throughput)

Substituting the Values:

Write Throughput =1100.4008415578

The estimated write throughput of the proposed algorithm I is 1100.400841558 Transactions/Sec.

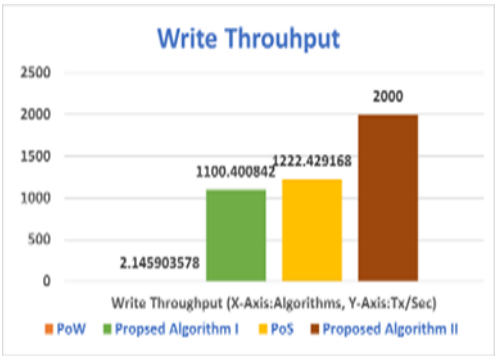

Figure 8: Comparison of Write Throughput

5.7 Average Write Latency

Write latency generally refers to the time it takes for data (in this case, a transaction) to be written to the blockchain after it is submitted to the network. This can include the time the transaction spends in the mempool (waiting to be included in a block) and the time it takes to propagate across the network. Write latency encompasses more than just the confirmation time, as it also includes any delay before the transaction is picked up by a miner.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 11, Issue 3, pp: (41-56), Month: September - December 2024, Available at: www.noveltyjournals.com

The average write latency can be written as Delay + Confirmation time

Where delay refers to the wait time in the memory pool and network delays etc.

Thus Average write latency in PoW systems is = Delay + Average confirmation time

= Delay + 8848.160393 Sec

And PoS systems is = Delay + Average confirmation time

= Delay + 14.00585277 Sec

Average Write Latency of the proposed algorithm I= Delay + 8862 Sec

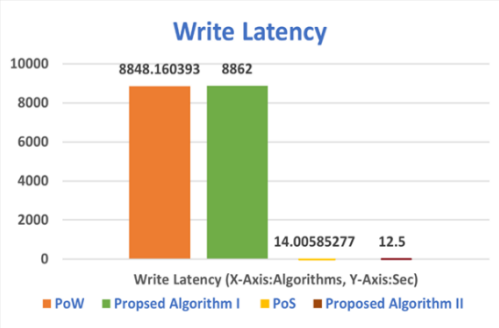

Figure 9: Comparison of Write Latency

5.8 Total Orphan Blocks/Uncle Blocks

Orphan/uncle blocks (or ommer blocks) are blocks that were mined almost simultaneously with another block, but were not included in the main blockchain. This can happen when two miners find a valid block at roughly the same time, but only one of these blocks will be included in the canonical blockchain, while the other becomes an uncle block.

The total number of orphan blocks in PoW = 376 blocks

The total number of uncle blocks in PoW = 1306719 blocks

The total number of uncle blocks in the proposed algorithm I = 0 blocks as of now (There is little simulation data available)

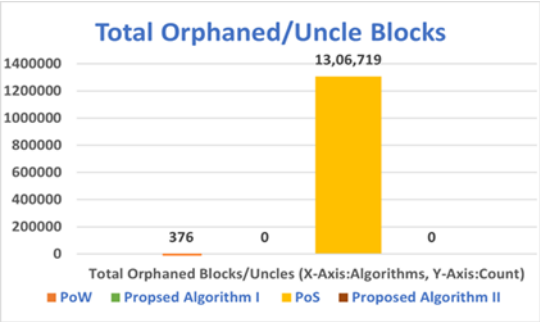

Figure 10: Comparison of Orphan/Uncle Blocks

5.9 Success Rate

Success rate refers to the total number of blocks created to that of the total number of blocks available in the actual blockchain

i.e. Success Rate = Total blocks mined (Available in actual blockchain + orphan blocks) *100/ Total blocks available in actual blockchain

For PoW, Success Rate = 856570 *100 /(856570+376)

= 99.95612326%

For PoS, Success Rate = 20518689/(20518689+1306719)*100

= 94.01285419%

For the Proposed algorithm I, Success Rate = 100% as of now (There is little simulation data available)

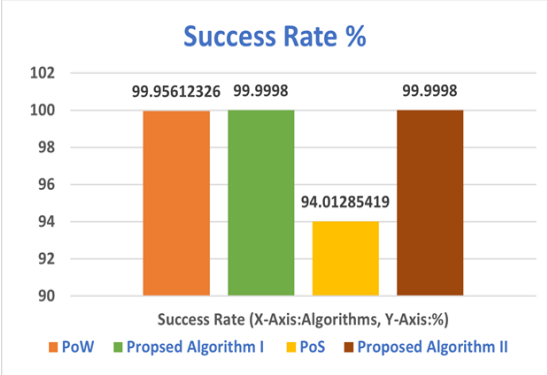

Figure 11: Comparison of Success Rate

5.10 Security

The proposed algorithm I: By using constrained computing resources, the suggested method seeks to address issues including double-spending, 51% attacks, biased miner selection, and forking. It solves the issue of long transaction confirmation times and offers robust security independent of the attacker's computing power or cash holdings.

This model ensures unbiased miner selection and provides an effective defense mechanism against current attacks while being capable of detecting and mitigating future threats.

Proposed Algorithm II: The rich-getting-richer syndrome can be mitigated as there exists another parameter called timestamps of staked tokens and they reset on every election. There is no requirement for a validator to wait for 30 days before being able to participate in the next election after winning one. There is no requirement for validator tokens to be at stake for a minimum of 30 days to be able to participate in the election. This approach results in a more randomized and fair selection of validators.

The precision and randomness can be improved with the help of the proposed methodology. These two factors significantly influence the selection of validators, effectively decreasing the "rich-getting-richer" phenomenon and thus satisfying the true decentralization concept.

The summary of the analyzed metrics is given in the below table.

Table 2. Consensus Protocols comparison

S.No	Metrics	PoW	Proposed Algorithm I	PoS	Proposed Algorithm II
1	Average Block Size (KB)	1536	3072	1024	1024
2	Average Confirmation Time (Seconds)	8848.160393	8862	14.00585277	12.5
3	Average Difficulty (TH)	11781764142115.50	589088208538.46	2865.364813	0
4	Average Network Hash Rate (MTH)	85722488.23	8572249.043	0.0002207	0
5	Network Utilization (%)	78%	59.60%	57.55%	50.62%
6	Average Transaction Fee (Dollars)	7.099420537	NA	4.873568616	NA
7	Total Orphaned Blocks/Uncles (Count)	376	0	1306719	0
8	Write Throughput (Tx/Sec)	2.145903578	1100.400842	1222.429168	2000
9	Success Rate (%)	99.95612326	100	94.01285419	100

The summary of the attacks and other parameter comparisons is given in the below table.

Table 3. Consensus Protocols Attacks and other parameters comparison

S.No	Parameters	PoW	Proposed Algorithm I	PoS	Proposed Algorithm II
1	51 % Attack	High	Solved	Medium	Solved
2	Unfair Miner Selection	High	Solved	High	Solved
3	Forking Issue	Low	Low	High	Low
4	Double Spending Problem	Low	Low	Low	Low
5	Rich Getting Richer Syndrome	High	Solved	High	Solved
6	Validator Waiting Time	Low	Low	Low	Solved
7	Energy consumption	High	Medium	Low	Low
8	Randomization of Validators	Low	Solved	Low	Solved
9	True Decentralization	Low	Solved	Low	Solved

6. CONCLUSION

An exhaustive survey has been done regarding the recent and mostly used consensus algorithms across various domains. There are many limitations and drawbacks associated with these consensus algorithms. The main motivation of this research is to design an efficient and secure consensus algorithm that can be used in public blockchains. As part of the research, two new consensus algorithms were proposed which were presented in sections 3 and, 4 and the analysis of the proposed algorithms is presented in section 5.

The proposed algorithms were analyzed thoroughly and compared with the existing (most widely used) consensus algorithms with respect to performance and security metrics and the proposed algorithms clearly have better decentralization level, security against attacks and performance.

REFERENCES

[1] Haber, Stuart; Stornetta, W. Scott (January 1991). "How to time-stamp a digital document". Journal of Cryptology. 3 (2): 99–111. CiteSeerX 10.1.1.46.8740. doi:10.1007/bf00196791. S2CID 14363020.

[2] S. Nakamoto, ‘‘Bitcoin: A peer-to-peer electronic cash system,’’ White Paper, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] M. Swan, Blockchain, Blueprint for a New Economy. Sebastopol, CA, USA: O’Reilly Media, 2015.

[4] J. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed. Indianapolis, IN, USA; Wiley, 2008.

[5] B. Schneier, Applied Cryptography, Protocols, Algorithms and Source Code in C, 2nd ed. Hoboken, NJ, USA: Wiley, 1996.

[6] L. Lamport, ‘‘Password authentication with insecure communication,’’Commun. ACM, vol. 24, no. 11, pp. 770–772, Nov. 1981.

[7] C. R. Merkle, ‘‘Method of providing digital signatures,’’ U.S. Patent 4 309 569, Sep. 5, 1979.

[8] Y. Lu, ‘‘Blockchain: A survey on functions, applications and open issues,’’ J. Ind. Integr. Manage., vol. 3, no. 4, Dec. 2018, Art. no. 1850015.

[9] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, ‘‘A survey of blockchain technology applied to smart cities: Research issues and challenges,’’ IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2794–2830,Feb. 2019.

[10] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, ‘‘Integrated blockchain and edge computing systems: A survey, some research issues and challenges,’’ IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019, doi: 10.1109/COMST.2019.2894727.

[11] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, ‘‘The blockchain as a decentralized security framework [future directions],’’ IEEE Consum. Electron. Mag., vol. 7, no. 2, pp. 18–21, Mar. 2018.

[12] Y. Xinyi, Z. Yi, and Y. He, ‘‘Technical characteristics and model of blockchain,’’ in Proc. 10th APCA Int. Conf. Control Soft Comput. (CONTROLO), Jun. 2018, pp. 562–566.

[13] D. Massessi. Blockchain Consensus and Fault Tolerance in a Nutshell. Accessed: May 12, 2019. [Online]. Available: https://medium.com/coinmonks/Blockchain-consensus-and-fault-tolerance-in-a-nutshell-765de83b8d03

[14] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, ‘‘Decentralized applications: The blockchain-empowered software system,’’ IEEE Access, vol. 6, pp. 53019–53033, 2018, doi: 10.1109/ACCESS.2018.2870644.

[15] E. J. A. Kroll, ‘‘The economics of Bitcoin mining, or Bitcoin in the presence of adversaries,’’ in Proc. 12th Workshop Econ. Inf. Secur. (WEIS). Washington, DC, USA: Georgetown Univ., 2013, p. 11.

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

[17] P. Vasin. (2018). Blackcoin’s Proof-of-Stake Protocol V2. Accessed: Mar. 20, 2019. [Online]. Available: https://blackcoin.co/blackcoin-pos-protocolv2-whitepaper. Pdf

[18] “Proof of Stake versus Proof of Work White Paper.” (2016).

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

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

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

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

[23] P. Rajitha, D. Ramya, “Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain,” in Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021.

[24] D. Larimer, ‘‘DPOS consensus algorithm—The missing white paper,’’Steemit, New York, NY, USA, White Paper, 2018.

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

[26] Anjaneyulu Endurthi, Akhil Khare, “An Efficient and Robust Proof of Stake Algorithm Based on Coin-Age Selection”, Journal of Theoretical and Applied Information Technology, 2024.