IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

*Digital Object Identifier Doi Number*

# MBCP: Performance Analysis of Large Scale Mainstream Blockchain Consensus Protocols

**MANPREET KAUR[1, 2], MOHAMMAD ZUBAIR KHAN[3], SHIKHA GUPTA[1], ABDULFATTAH NOORWALI[4], CHINMAY CHAKRABORTY[5], and SUBHENDU KUMAR PANI[6]**

[1]Department of Computer Science & Engineering, University Institute of Engineering, Chandigarh University, Gharaun,140413, Punjab, INDIA
[2]Department of Computer Science and Engineering, Guru Nanak Dev Engineering College, Ludhiana, 141006, Punjab, INDIA
[3]Department of Computer Science, College of Computer Science and Engineering, Taibah University, Madinah 41477, SAUDI ARABIA
[4]Department of Electrical Engineering, Umm Al-Qura University, Makkah, SAUDI ARABIA
[5]Department of Electronics and Communication Engineering, Birla Institute of Technology, Mesra 814142, Jharkhand, INDIA
[6]Principal, Krupajal Computer Academy, BPUT, Odisha, INDIA

Corresponding author: Manpreet Kaur (e-mail: preetmand@gmail.com), Chinmay Chakraborty (e-mail: cchakrabarty@bitmesra.ac.in).

The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: 19- ENG-1-01-0015.

**ABSTRACT** As Blockchain innovation picks up popularity in many areas, it is frequently hailed as a sound innovation. Because of the decentralization and encryption, many imagine that data put away in a Blockchain is and will consistently be protected. Among various abstraction layers of Blockchain architecture, the consensus layer is the core component behind the performance and security measures of the Blockchain network. Consensus mechanisms are a critical component of a Blockchain system's long-term stability. Consensus forms the core of blockchain technology. Therefore, a range of consensus protocols has been introduced to maximize Blockchain systems' efficiency and meet application domains' individual needs. This research paper describes the layered architecture of Blockchain. A comprehensive review of mainstream consensus protocols mainly Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Activity (PoA) is presented in the paper. These mainstream consensus protocols have been explained and detailed performance analysis of these consensus protocols has been done. We have proposed a performance matrix of these consensus protocols based on different parameters like Degree of decentralization, Latency, Fault Tolerance Rate, Scalability, etc. Consensus protocols being the core of a strong fault-tolerant secured blockchain system, the proposed work intends to help inappropriate protocol selection and further research on strengthening trust and ownership in the technology. Depending upon different parameters like decentralization which is low in POA compared to other protocols, whereas POW is non-scalable, so depending on the priority of a particular performance parameter, the paper will help in the selection of a specific protocol.

**INDEX TERMS** Blockchain, PoW, PoS, DPoS, PoA, Consensus Protocol.

## I. INTRODUCTION

Nowadays, Blockchain is considered one of the most quickly-growing technologies, and it has been becoming increasingly popular due to its unique features. Satoshi Nakamoto [4] demonstrated the method in which Blockchain technology, a cryptographically secured P2P connected network, could effectively be utilized to get rid of various issues related to transaction management in chronological order and to prevent the double-spending problem. Blockchain technologies are continuously surprising the world to a great extent because of the successful accomplishment of Bitcoin [28]. It is possible to describe Blockchain as a public open ledger spread over many nodes that do not inherently trust each other. These nodes adopt an append-only data structure, i.e., new data and transactions can only add to Blockchain, but previous data remain intact. Consensus methods are the heart of any Blockchain application, so the chosen consensus protocol

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3085187, IEEE Access



should meet that particular application's requirements. This paper reviews the existing consensus mechanism for Blockchain systems and analyzes their performance and security features.

### A. STATEMENT OF CONTRIBUTION

In this paper, we have discussed the blockchain architecture in the context of various layers of a blockchain framework, and then we have elaborated the consensus layer of this architecture to explore possibilities of improving the performance of the blockchain ecosystem. The consensus layer acts as the backbone of a blockchain application. Therefore scope to improve the performance of the blockchain system depends entirely on the underlying consensus mechanism. In this context, we present four mainstream consensus protocols namely PoW, PoS, DPoS, and PoA. These consensus protocols are further demonstrated using either pseudocode or flowchart. A comparison in terms of the advantages and disadvantages of each consensus mechanism has been provided. The performance of these consensus mechanisms has been evaluated based on parameters chosen from the existing literature. Our main contribution is the detailed explanation on all these protocols with pseudocode(s) or flowcharts and a performance matrix being designed after analyzing these consensus methods against the parameters chosen.

### B. OUTLINE OF PAPER

This paper is organized as follows. Section I contain the introduction of the blockchain to provide a general idea about the technology. Section II presents the survey of existing literature related to the blockchain. The next Section III provides an overview of blockchain architecture. The characteristics of this architecture have been listed in the next section. The mainstream consensus mechanisms have been explained comprehensively in Section V with pseudocode or diagrammatic illustrations. In the next section, a performance matrix has been provided for these consensus methods with a list of performance evaluation parameters. Finally, Section VII concludes this paper.

## II. LITERATURE REVIEW

A consensus process is an agreement that guarantees that all parties in the ecosystem of Blockchain have to adhere to certain predetermined rules and regulations that make Blockchain a trustless, secure, and convenient technology. Different consensus protocols adopt different standards, allowing participants in the network to comply with certain policies and procedures. Interestingly, the common consensus mechanisms used by the financial institutions are Proof of Work (PoW), Proof of Stake (PoS) and Delegated Proof of Stake (DPoS). Yiang et al. [19] highlighted the five-component consensus protocol architecture and clarified the fault tolerance of different consensus protocols in distributed systems and transaction processing capabilities. A summary of DAG-based consensus approaches was also proposed in this paper by the authors. They define four classes of consensus methods based on PoS and present computational abstraction for each class. The paper by Leila et al. [12] is one of the research surveys arranged to provide detailed information about consensus methods. This paper has divided the Blockchain architecture into three classes such as single layer and multi-layer-based Blockchain architecture and interoperability-Based architecture. The authors further explained existing use cases based on Blockchain and addressed some issues and possible solutions. The paper [15] has provided a detailed description of five consensus protocols PoW, PoS, DPoS, PBFT, and Ripple. Wang et al. [33] define the Blockchain's most familiar consensus algorithm as the PBFT. But, it has established the issues of reliability in the PBFT and huge resource requirements faced by the systems. A new credit-delegated byzantine fault tolerance (CDBFT) consensus protocol was therefore formulated in this paper, which assigns a credit reward for each newly created block to the node. The simulation has been performed, which represents the reduced communication overhead and the improved efficiency. The PoS based on coinage comes out to be a better alternative to PoW used by earlier Bitcoin implementation due to sound security provisions provided at low transaction fees by this hybrid design, as demonstrated by King et al. [20]. To enhance communication among the Blockchain network partners, the PREStO systematic framework has been created [17]. The paper designed a BLOCKBENCH system for the study of private Blockchain performance. They have discussed the detailed description of various layers of Blockchain architecture [10]. In this work [42] presented a modified consensus approach called 2 hop consensus for public blockchain, in which repeated rounds of PoW and PoS have been employed to reduce the effect of 51 % attack and double-spending attack to nearly impossible. Moreover, this paper divides the consensus methods into two classes namely proof-based and voting-based methods. The survey conducted by Bamakan et al. [34] has categorized major performance metrics into four different categories via algorithm throughput (TPS, Block Size, latency, verification time), mining profitability (rewards, power consumption, Transaction fee), degree of decentralization, and securities and vulnerabilities(51% attack, sybil attack, double spending attack). A recent survey had discussed [29] the utilization of state of art consensus mechanisms. In this work, they have identified the PoW to be the most commonly used algorithm with 57% usage and DPoS to be the second most used algorithm with 11% and then PoS is secured at third position with 6% usage among analysis of top 100 cryptocurrencies around the world. The systematic review of the key public consensus process relevant to Blockchain technology is included in this paper, and several papers have been reviewed in this context. Through this paper, as shown in Fig. 1, we covered the study of Blockchain architecture, and we elaborated the consensus layer of this architecture to understand the underlying better mechanism to reach the agreement of whether to include or discard a particular block. The method of doing this largely depends upon the underpinned style chosen for the consensus algorithm.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3085187, IEEE Access



Therefore, to further narrow down our research, we have selected four mainstream consensus techniques: Proof of Work, Proof of Stake, Delegated Proof of Stake, and Proof of Activity. Also, we have presented the merits and demerits of these consensus methods. In the end, we also evaluated the performance of these four techniques concerning some evaluation metrics.

## III. BLOCKCHAIN ARCHITECTURE

Blockchain architecture, as seen in Fig. 2, comprises of following five abstraction layers used in most of the existing applications [35].

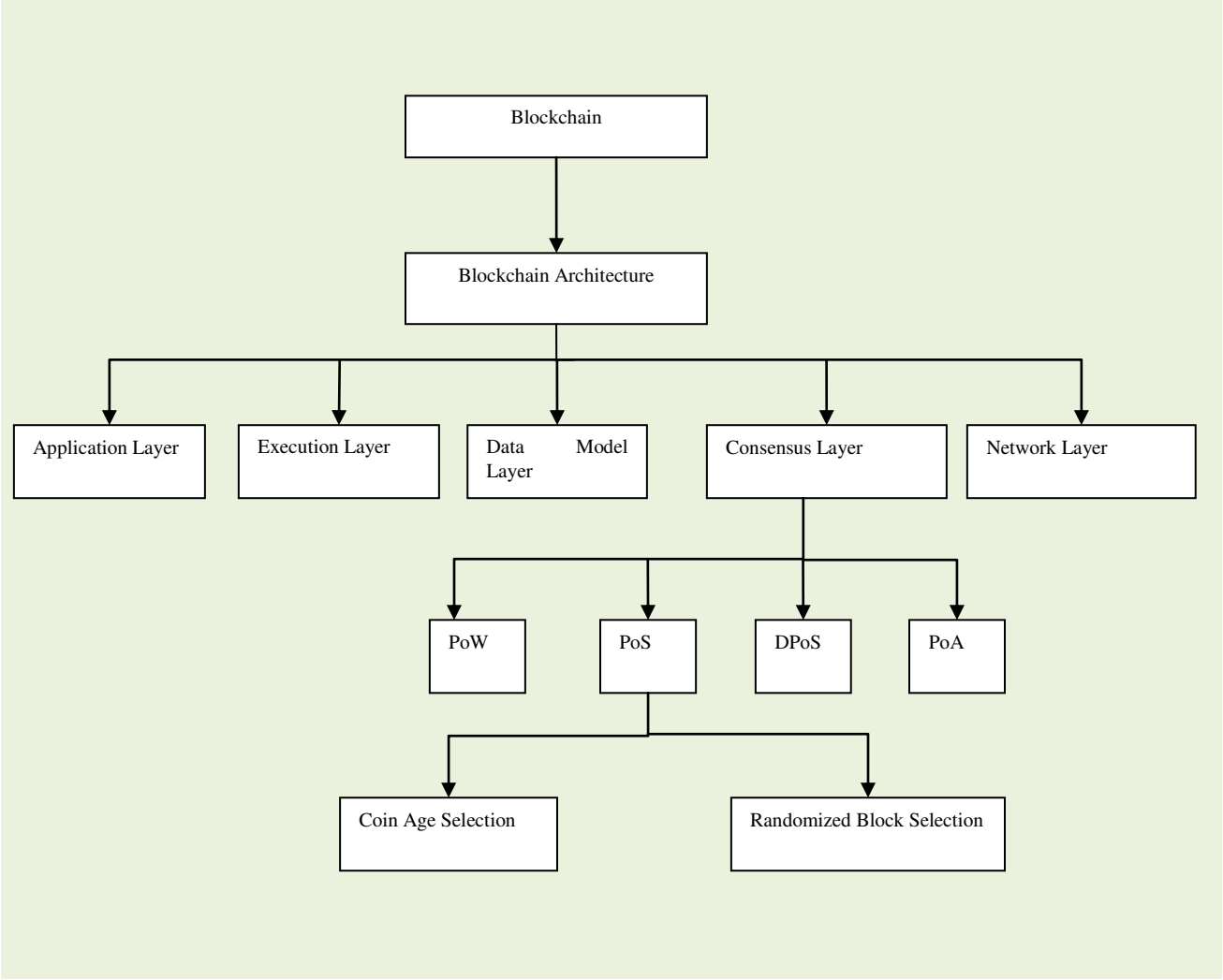


**FIGURE 1. Overview of Blockchain Architecture reviewed in the paper**

### A. NETWORK LAYER

The communication of blocks between various participating blockchain network entities is the responsibility of the P2P network layer. This particular layer is accountable for the transmission of data among various participants of a network. Each Blockchain system has a P2P network that is built on its network topology and peer behavior, determined by the feedback from the client software and the actions of the end-user [5]. A Peer-to-peer network behaves like a gossip network where everyone tells the information to other people, and eventually, everyone gets the message in the network [7] [46].

### B. CONSENSUS LAYER

This is one of the most crucial layers present in all standalone Blockchain. This layer ensures that the blocks to be added in the correct sequence should adhere to the blocks' validity to be added by peers in the system. The PoW (Proof of Work) protocol utilized by Bitcoin and PoS (Proof of Stake) [2] are common examples. The consensus layer's function is to get the information provided and stored by the Blockchain to be accepted by all nodes in the system. In other words, this layer guarantees that upon validation, if a block is being appended by one node, then that same block is being appended by every other node in their copy of Blockchain [10]. Hence, the role of the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3085187, IEEE Access



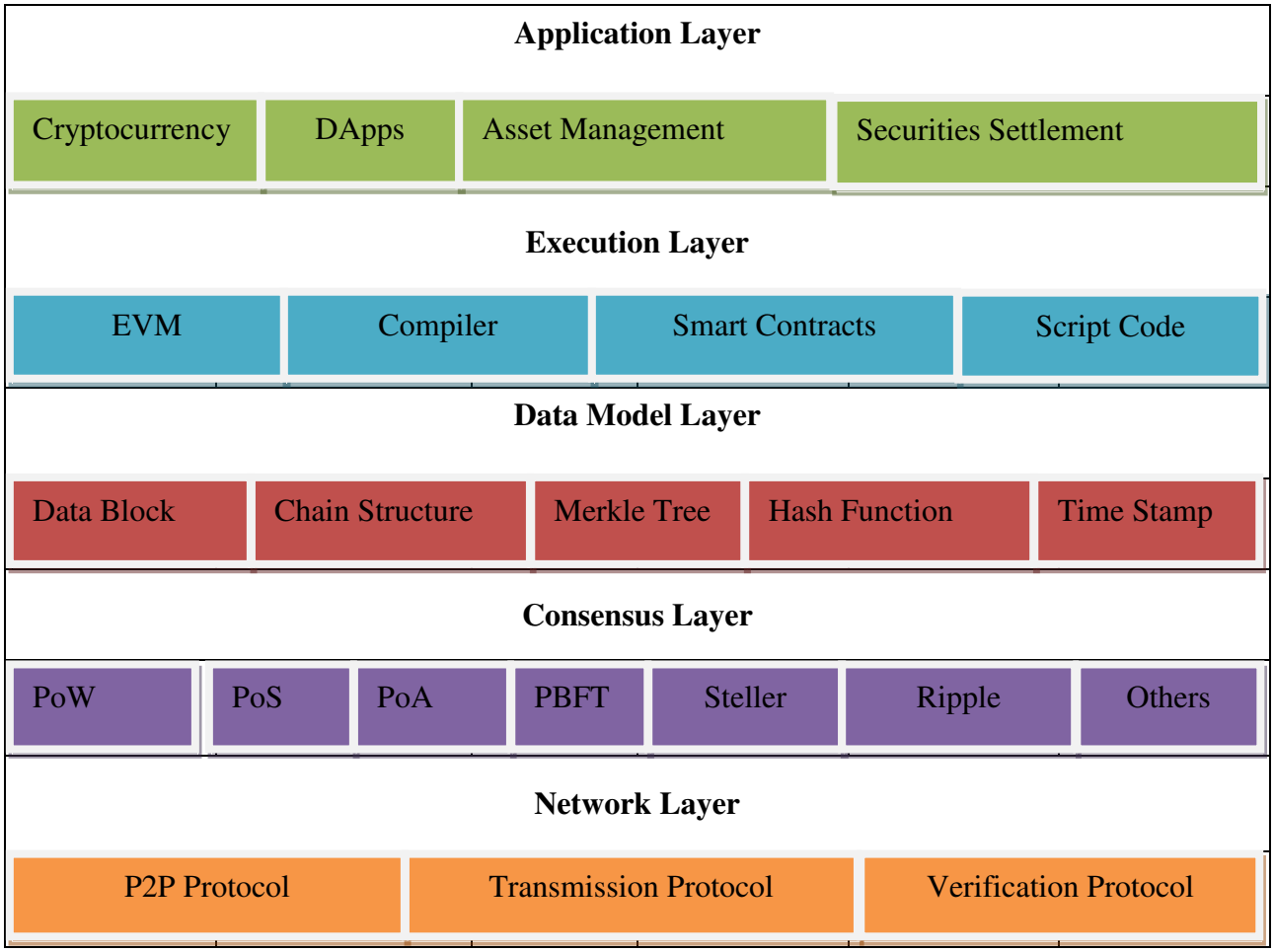


**FIGURE 2.** **Blockchain High-Level Architecture Layers**

consensus layer is to get mutual agreement on data stored in a block from all participating nodes in the Blockchain system. Therefore whenever any block is being appended in Blockchain, it requires network approval [45][47]from the participating nodes on the block content. In the consensus layer, there are numerous protocols with which a block is deemed validated and attached to the Blockchain. This layer deals with integrating the data model layer in Blockchain to create, validate and add a new block [22]. The data model layer deals with block layout and its lower layer deals with the "consensus process" used to construct and validate the new block of Blockchain. Inside the current Blockchain scenario, the PoW consensus algorithm is the most widely employed method, certainly in cryptocurrencies. Various other commonly used consensus algorithms are PoA, PoS, PBFT, Delegated Proof of Stake (DPoS), and many more [8].

### C. DATA MODEL LAYER

This layer defines the data model and physical storage used by Blockchain. Blockchain's distributed ledger is a form of transparent and self-regulating open-source database replicated and coordinated through several locations to carry out and track transactions [38]. This ledger is constructed using a linked list of blocks that have been encrypted with asymmetric encryption or Merkel trees [9]. The layer provides the layout, content, and functions performed by information stored in a block. In general, a block can be seen as a collection of transactions and a set of predefined scripts executed, as well as their latest instances [10]. Each block is mathematically identified by its content's digital signature and a reference to the ancestor block's hash. Cohesively, all blocks create a distributed ledger or Blockchain. In a Merkel tree, transaction hashes that are stored in a block are packed together. Every component and utility in the Blockchain network is an essential aspect of this innovation and is intended to ensure that transactions can be made, distributed, approved, and eventually stored in the Blockchain.

### D. EXECUTION LAYER

Through the aid of smart contracts, the execution layer implements trust [3]. The concept of smart contracts came into existence with Ethereum. Each Blockchain node has a

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3085187, IEEE Access



local virtual machine named EVM, i.e., "Ethereum Virtual Machine" in Ethereum. Smart Contract is a code or group of programs that run on EVM [11]. A smart contract collects self-executing computer instructions to ensure mutual consent between non-trusting parties [25]. Miner nodes automatically invoke their deployment and execution as a part of Blockchain transactions. The execution module supports all the processing environment details and requirements that support Blockchain operations [10]. Within this processing set - up, a contract (or chain code) is executed. One of the Blockchain application's common requirements is the execution process's speed, as different contracts and transactions are stored in one block, and all should be confirmed by the node [39]. Another prerequisite is to obtain probabilistic execution, consistent at all nodes, ideally. Probabilistic execution removes unwanted uncertainty in the input and output of operations, which certainly prevents discarding or aborting the blocks [48]. As in PoW, it leads to a waste of considerable computing resources due to aborted transactions.

### E. APPLICATION LAYER

There are numerous applications in the application layer that client users use to communicate with the Blockchain framework. Scripts, APIs, user interfaces and frameworks are included in this layer. The Blockchain network acts as a back-end framework for these apps, and clients also link through APIs to the Blockchain system. The Blockchain records are irreversible and open to the participants, which ensure that they can never be altered once a record is incorporated, and this aspect promotes the integrity of data. Therefore, cryptocurrencies are the most comprehensive Blockchain application to date. Different Blockchain applications' business strategy is also included at this layer that can vary from application to application [8].

## IV. BLOCKCHAIN ARCHITECTURE CHARACTERISTICS

a) Decentralization- The majority of participating nodes must agree to execute and validate Blockchain transactions [39]. On all the nodes in a ledger, these transactions are reproduced. This removes the need for transaction data to be exchanged and retained by intermediaries [13].

b) Immutability- Hash values are unique for every block. Each block contains a hash address itself and the hash address of its preceding block. If any node attempts to change block data, it has to alter data everywhere as blocks are spread worldwide. Additionally, it has to change all the blocks as change in one block will generate a different hash value, making all subsequent blocks invalid. Hence every subsequent block strengthens the verification of the previous block in Blockchain. Therefore, data on the Blockchain will never be altered in an existing block, making it irreversible and tamper-proof [41].

c) Transparency- The distributed ledger is modified only if the majority of the entities reach mutual consent. Moreover, to ensure transparency and security, the networks' modifications are publicly noticeable [36].

d) Traceability- Blockchain's open and decentralized nature facilitates the backtracking of every transaction activity. It is possible to track each update in an asset's state back to its roots. It serves to create the network more stable, effective, and straightforward.

e) Trustless- Blockchain enables asset transfers among untrustworthy nodes. Consistency and integrity of transactions are maintained in a trustless environment by replicating records across several network nodes and obtaining consent from participating nodes [36].

## V. CONSENSUS MECHANISM

These consensus algorithms are the center of Blockchain technology. Consensus seeks to reach agreements according to the network entities' needs between network nodes or systems. The tool for maintaining transaction reliability and validity is the Consensus algorithm. PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated PoS), PoA (Proof of Activity) are the most common consensus algorithms used by public Blockchain applications. However, the cost of computing, protection and consensus efficiency of the above are all unique. A thorough overview of conventional consensus processes is given in this section.

### A. PROOF OF WORK (PoW)

Dwork and Naor first reported the proof of work (PoW) in the early 1990s, and Nakamoto used it in a "Bitcoin paper" in 2008 [14]. PoW is the first popular method of consensus. Many high-level financial organizations have used PoW. In PoW, all nodes must compete with their computational power to create a valid block of transactions. In this contest, a cryptographic puzzle must be solved by the participating nodes. All blocks have a value called a nonce. The miner must obtain a nonce value to protect the block, as the cryptographic value of the entire block should fall below a predefined threshold (called weight) [39]. This would increase the computational complexity of mining. The privilege to build a new block may be granted to a miner node that begins to solve a puzzle. Resolving a PoW puzzle is complicated. The transaction fee is associated; however, the service provider calculates its amount. The "mining fee" is also paid by the entire Blockchain network to the miner [12, 29].

The strengths of using this approach are primarily expressed in the protocol's fairness. If a miner's computational resources contribute to "x percent" of the system's cumulative resources, then the miner has a relatively x likelihood of generating blocks and getting paid. To build blocks that are "useful" to the intruder, the intruder's computing resources must compete with other

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3085187, IEEE Access



"trustworthy nodes" of the entire system. From its inception, the PoW algorithm has been attributed to the success of "Bitcoin" [16]. Another advantage of PoW is the complexity of solving the computational puzzle [12]. While PoW can ensure data consensus, it takes approximately ten minutes to create a block, and too many processing and energy resources are used for this challenge [33]. It also suffers from several drawbacks. One of the major problems is known as the 51 percent attack. A 51 percent attack, or majority attack, is a situation where most computing power is owned by a miner or a pool of miners. Besides, it benefits the wealthy, as a miner's likelihood for block mining is linear concerning the computing capabilities owned by that miner. Therefore, another consensus mechanism, PoS, has been proposed [17]. Pseudocode for typical PoW is shown in Fig. 3.

**The pseudocode of a typical Proof of Work mechanism**:
Start
INPUT: Block_header (prev_block_hash, merkle_root, time_stamp), nonce, difficulty_value
Output: Fixed size valid block hash: Block_hash
1. Init n= nonce
2. // compute block hash for current block
   Compute Block_hash = SHA256 (Block_header (prev_block_hash, merkle_root, time_stamp), n)
3. if (Block_hash <= difficulty_value) //Valid Block hash found
4. then Write block into blockchain // Broadcast Block to Blockchain Network
5. end
6. else //Block hash invalid
7. Set n = n+1 // adjust nonce to some new random value
8. Goto step 2
   Stop

**FIGURE 3.** **Pseudocode of a typical Proof of Work**

### *B. PROOF OF STAKE (PoS)*

Proof of Stake (PoS) was introduced in 2011 and utilized by cryptocurrency "Peercoin" in 2012. In PoS, the miner termed as the "forger", and "mining process" can be described as forging [40]. Each forging node deposits as a stake a specific portion of the possessed digital currency in the system at the preliminary phase, which the protocol uses to identify the next forger in the system [12].

There are two strategies for choosing forgers in PoS [40]:

1) Selection of the coin-age.
2) Randomized block selection

#### 1) COIN-AGE SELECTION

In the selection process for coin-age pseudocode shown in Fig.4., as shown in pseudocode the node with the highest coin-age value called forger to add blocks in the network is chosen [12, 22]. The coinage is determined as a product of the number of coins and accumulation time in days [40, 22].

For instance, two coins accumulated for 30 days will have a coinage of 60 coin-days, i.e. (2 × 30) [12].

#### 2) RANDOMIZED BLOCK SELECTION

Randomized block selection method: In this approach [21, 40], as seen in the pseudocode presented by Fig.5, a forger with a particular value called "hit value" is chosen to generate a new block. Any forger encodes the hash of its ancestor block by using its secret key to calculate "hit value" [12, 40].

The encrypted value is hashed, and the initial 64 bits of this hashed value are extracted as hit value. In the calculation, each forger uses a private key to determine a distinct hit value. A forging node with a hit value not exceeding the "target value" is chosen for the forging [12]. Using (1), the target value is obtained.

$$T = T_b \times L \times S_e \qquad (1)$$

where

a) $T_b$ = "base target value" = previous block target value × time consumed to forging that block.
b) L = time elapsed since the last block forged.
c) $S_e$ = amount of coins accumulated or staked [12].

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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3085187, IEEE Access



**FIGURE 4.** **Pseudocode of PoS (Coin-Age Selection)**

**The pseudocode of a Proof of Stake (Randomized block selection) mechanism:**

```
Start
INPUT:  Block_header (prev_block_hash), target value, forger_pool
Output: Fixed size valid block hash: Block_hash
      //Select forger with particular target value
1.    Init c=0
2.    Array selected_node[size_of_forger_pool]
3.    For every forger i in forger_pool
4.    // compute hash value from previous hash value of block  and forgers's private key
5.    Compute H_i = SHA256(prev_block_hash, private_key_i)
6.    hit_value_i = substring (H_i , 0, 64) //extract initial 64 bits as hit value
7.    // Compare hit value with target value
      If (hit_value_i<= target_value)
8.    Then selected_node[s]= forger_i
9.    Set c=c++
10.   End if
11.   End for
12.   If (size(selected_node)>1)
13.   Then
14.   For every node n in array selected_node
15.   Calculate difficulty_level of every node
16.   Return node f as Forger whose difficulty level is maximum
17.   Grant block write permissions to node f
18.   Endfor
19.   Else if (size(selected_node)=1)
20.   Grant block write permissions to selected_node
21.   Else
22.   Return false // wait for either other nodes to became forger or adjust target value
Stop
```

**FIGURE 5.** **Pseudocode of PoS (Randomized block selection)**

If there is more than one forger with a hit value not exceeding the "desired target value," then the forger is chosen whose difficulty level is relatively high. As specified in (2) [12], the cumulative difficulty is determined as described. If peers validate a block in the network, the block forger will collect a transaction fee as a reward for all the transactions. In PoS, mining charges are excluded. On the contrary, the staked coins are lost when the forger tries to create a malicious block, which will protect the system against malicious attacks.

$$D_{cb} = D_{pb} + \frac{2^{64}}{T_b} \qquad (2)$$

where $D_{pb}$ is the difficulty of the previous block and $D_{cb}$ is the difficulty of the current block.

### C. DELEGATED PROOF OF STAKE (DPoS)

This method is an extension of the conventional PoS mechanism. This approach is representative democratic, unlike PoS, which is solely democratic [13]. In 2014, Larimer proposed the Delegated Proof of Stake (DPoS) to fix the rich's problem of becoming richer in the PoS [12, 24]. It can be done by choosing delegates based on a voting decision instead of a coin stacking measure [40]. A group of nodes in a network (known as delegates) are selected in the DPoS, similar to the election mechanism. Every node in the system that owns cryptocurrencies contributes to the voting phase [12, 40]. The sum calculates the worth for vote of a node of coins staked [12]. As in (3), W ($N_V$) is the weight of node vote, and $B_e$ is coin stacked by the node.

$$W(N_V) \propto B_e \qquad (3)$$

It implies that to build and validate blocks, a delegate node is selected by voting 50% of the system's nodes. It enables speedy transactions but at the expense of the decentralization of Blockchain. It should be remembered that in this consensus process, there is a procedure to detect and vote out a malicious delegate [23, 43]. In a round-robin strategy, each delegate in the selected set of delegates will mine a new block created in the Blockchain. After a certain

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3085187, IEEE Access



period, the set of delegates would change. The successor delegate will then be chosen from that group if any delegate fails to create a block at a specific time [15]. DPoS, compared to

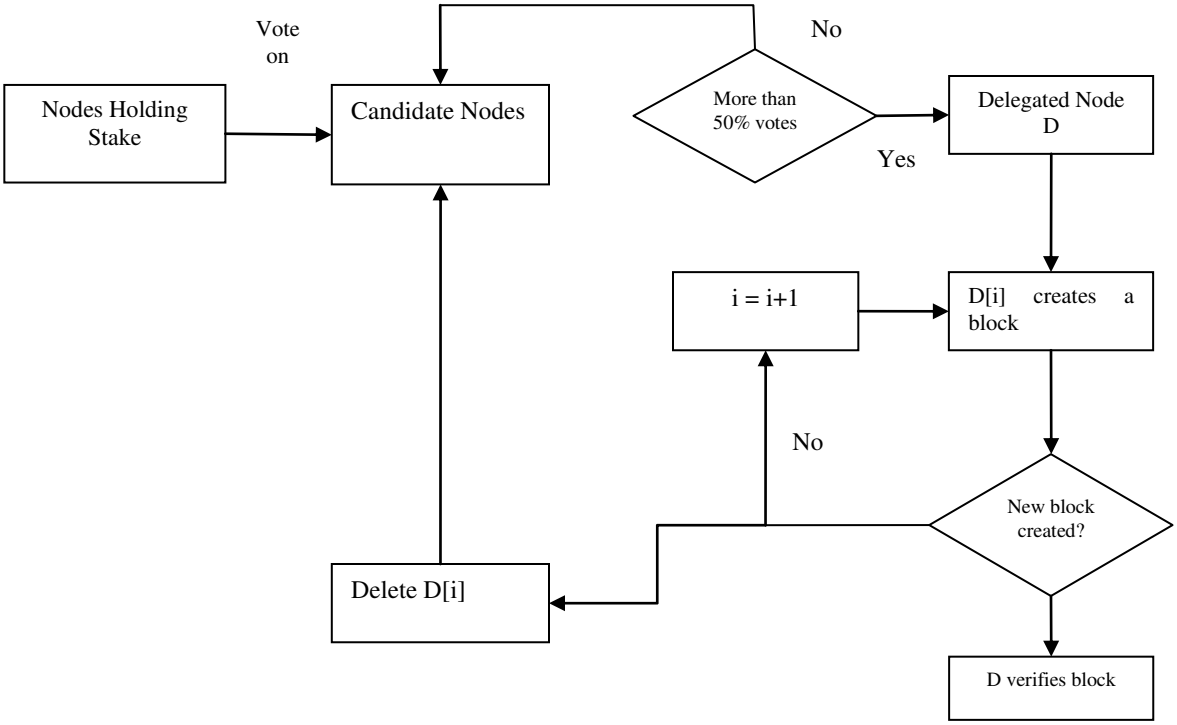


**FIGURE 6.** Delegated Proof of Work

PoW and PoS, is an inexpensive and better performance consensus protocol [15]. A virtual currency called BitShares uses this method of consensus.

### *D. PROOF OF ACTIVITY (PoA)*

To motivate miners to participate in the mining process and thus protect the system, miners receive a mining reward plus transaction fees in pure PoW [34]. 12.5 bitcoin is the current mining incentive and for every 210,000 blocks mined, it is halved. When the mining incentive is obsolete, the PoW becomes less relevant, and the miners depend only on the transaction fee [12]. As a result, miners dedicating their computing resources could lose their interest in actively engaging in the mining process and may require enormous transaction fees to mine the blocks. This is also due to the low value of transaction fees received compared to the high mining cost. Hence, these issues are addressed using an integrated approach based on PoW and PoS algorithms [12, 29]. This is done by splitting the fees for transactions between the miner and the validators (who are officially approved accounts), promoting the nodes' involvement, as shown in Fig. 7.

During the first phase, PoA works like pure PoW, with all the miners struggle to get a specific value of nonce necessary to produce a block [12, 40]. Here a miner indeed provides a block with header and address of the miner without payload. Then the miner will broadcast this created block to the network [29]. The following phase will choose "N validators" and term them as stakeholders based on the amount of cryptocurrency owned using the PoS algorithm. The block is confirmed and signed by of chosen stakeholder and broadcast into the network [44]. All chosen N-1 stakeholders sign the block before reaching the "Nth stakeholder" responsible for including the valid transactions in the block [12]. Therefore, this Nth stakeholder encrypts the block and broadcasts it to the network [12]. Transaction reward is distributed among miners who produced a block and the "N stakeholders" for the transactions included in the block [12, 40]. It is used by the cryptocurrency Decred [32].

We have also presented an analysis of these consensus algorithms' main advantages and disadvantages [18], under Table 1.

## VI. PERFORMANCE COMPARISON

The framework of comparison consists of different parameters based on their significance in defining the consensus protocols. Selected parameters which are applicability, Basis of assigning accounting rights, Degree of decentralization, Accounting nodes, Latency, Throughput, Fault Tolerance Rate, Overhead, Adversary Tolerance, Scalability, and Security are significant in analyzing the performance of these mainstream protocols. These parameters have been explained below in detail to

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3085187, IEEE Access



embark their significance in designing the protocols. We have compared protocols discussed so far via Table 2. We have also identified and analyzed various implementations of mainstream blockchain consensus mechanisms and compared these implementations against the selected performance evaluation parameters explained below.

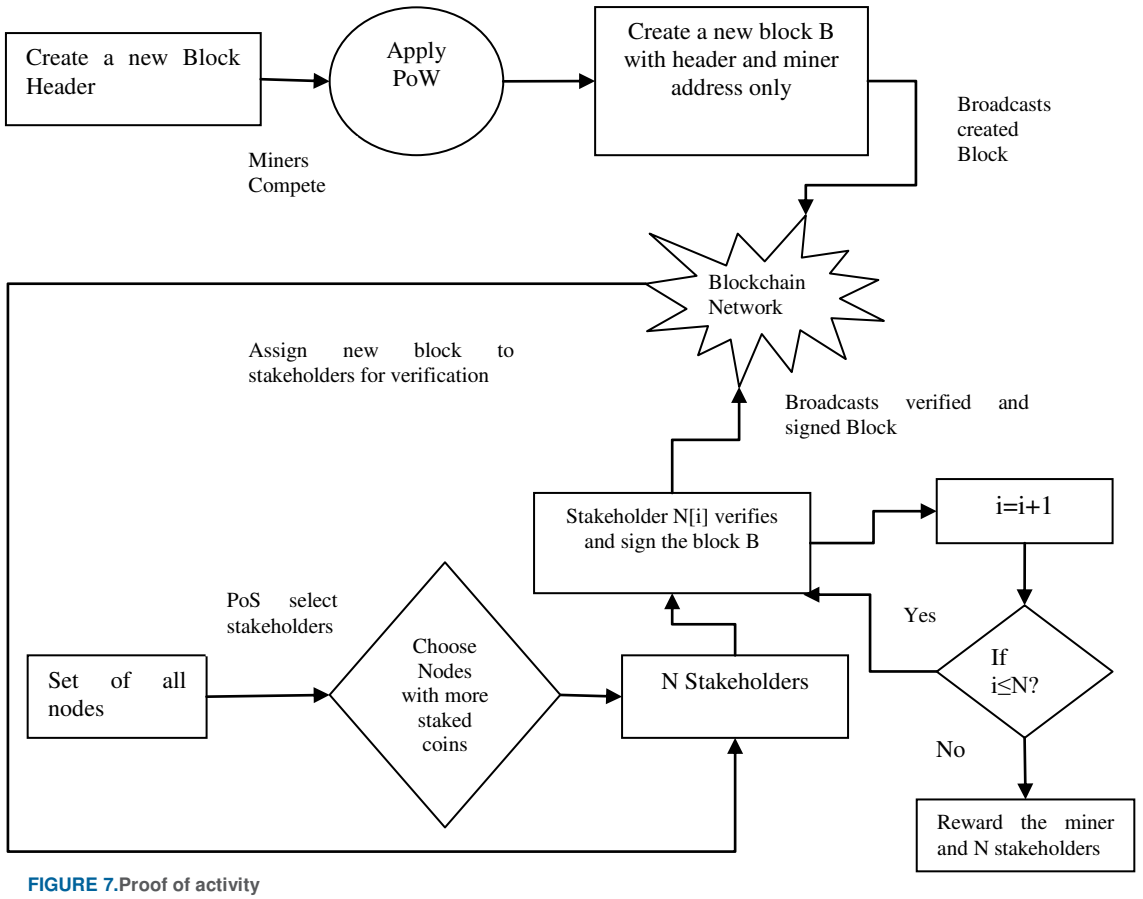


**FIGURE 7.** Proof of activity

- Applicability: Depending on the type of access control restriction applicable according to that consensus algorithm. Among the specified consensus mechanism the first three i.e. PoW, PoS and DPoS apply to public or permissionless blockchain systems. A public blockchain is an open network in which all transactions are visible to all participants and everyone could take part in a consensus mechanism. Whereas PoA method applies to private or permissioned blockchain. Interested nodes require membership or permissions to participate in the network. Since transactions are private and are only available to designated participants. Only those nodes that are associated with a particular enterprise would be allowed to take part in the PoA consensus mechanism.
- Basis of assigning accounting rights: The metric is based on which the accounting permissions are granted. In PoW, the permissions to take part in the consensus process are granted based on the computational resources available. In PoS and DPoS, rights to add block and participate in mining are based on degree of stake of nodes in the system. The activities performed are used to determine the rights to engage the nodes in consensus process.
- Degree of decentralization: It is the measure of the extent to which organizations want to decentralize their operation and decision-making powers. In PoA, PoS and DPoS consensus mechanisms the blockchain systems are fully decentralized as they are used by generally public blockchain systems. However, in PoA, decentralization is somewhat compromised as the nodes with high activity count can control the consensus process.
- Accounting nodes: It is the nodes that are held responsible for mining or creating new blocks. In

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3085187, IEEE Access



PoW and PoS, the whole network is held accountable for adding new blocks to the network as well as for mining of the blocks.

- Latency: It is calculated as the per-transaction response time. In Fig. 8, latency is presented of various consensus methods. Latency is metric that is based on transaction latency as well as block time, where transaction latency is the amount of time required for a transaction from its invocation to approval and block time is time required to mine a block as shown in Fig.10.

TABLE I
SUMMARY OF ADVANTAGES AND DISADVANTAGES OF BLOCKCHAIN CONSENSUS ALGORITHMS

| Consensus Mechanism | PoW | PoS | DPoS | PoA |
|---|---|---|---|---|
| Advantages | 1. Provides extensive decentralization of control in the network.<br>2. Highly Reliable. | 1. Relatively Fast.<br>2. Less energy consumption.<br>3. More efficient.<br>4. Better rewards with bigger stakes. | 1. Very less energy consumption.<br>2. Speedier operations than PoW, PoS and PoA.<br>3. Improved rewards distribution<br>4. Reduces hardware expenses. | 1. Increased fairness and efficiency.<br>2. Increased Safety.<br>3. Removes 51 percent attack [18].<br>4. Better topology of network.<br>5. Reduces transaction fees. |
| Disadvantages | 1. High energy and resource consumption.<br>2. Less efficient.<br>3. Time Consuming. | 1. More Costly.<br>2. Relatively more centralized than PoW.<br>3. Offers less safety than PoW. | 1. Large stake validators-rich people can dominate the system.<br>2. Fewer resiliencies due to less decentralization. | 1. Huge resource requirement.<br>2. The possibility to double sign transactions is available to stakeholders.<br>3. Hard to execute. |

A block contains a number of transactions as well. So it is measure of cumulative transaction time and mining period for every block. In general, PoW latency is approximately calculated as 10 minutes. In particular, Bitcoin provides the transaction latency of 60 minutes and Ethereum has found to be 6 minutes only. The average block time for above two implementations is 10 minutes and 12 seconds respectively. The PoS has much less latency equal to 1 minute only. In its implementation Peercoin the transaction latency is considered to be 5 minutes and in Cardano it is 10 minutes only. The average block time is 8 minute in Peercoin and 20 seconds in case of Cardano. DPoS has transaction latency of typically 3s in BitShares specifically. In Tron implementation of DPoS it is found to be 5 minutes. The average block time for Tron is 3 seconds and 1.5 seconds in BitShares, Finally, PoA has latency value 5 minutes and typically transactional latency of 30 minutes and average block time of 5 minutes for Decred cryptocurrency. Additionally, Fig. 11 depicts the latency of these mainstream consensus protocols.

- Throughput: It reflects the number of transactions a Blockchain system performs in a second. Before a transaction in a blockchain network can be processed, it must go through peer-to-peer verification [49]. With a larger number of users, this becomes time-consuming, particularly in a public blockchain network where each user validates the transaction. As a result, the number of transactions per second in a blockchain network exceeds the number of transactions per second (TPS) in traditional centralized networks. Developers and researchers have been working to improve the efficiency of blockchain technology in large-scale

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3085187, IEEE Access



applications. In Fig. 9. , the throughput capacity of various consensus methods is shown. The PoW implementations Bitcoin and Ethereum, in particular, have TPS of 7 and 15 respectively. In PoS the transaction rate is higher as in case of Cardano it is 250 and in Peercoin it could vary from 8 to 10. If the underlying consensus approach is DPoS then TPS gradually increases to 2000 in Tron and 3400 in BitShares. In the context of PoA (Decred) the number of transactions per second is 14 only. Among these consensus implementations, DPoS is much higher TPS as compared to other methods.

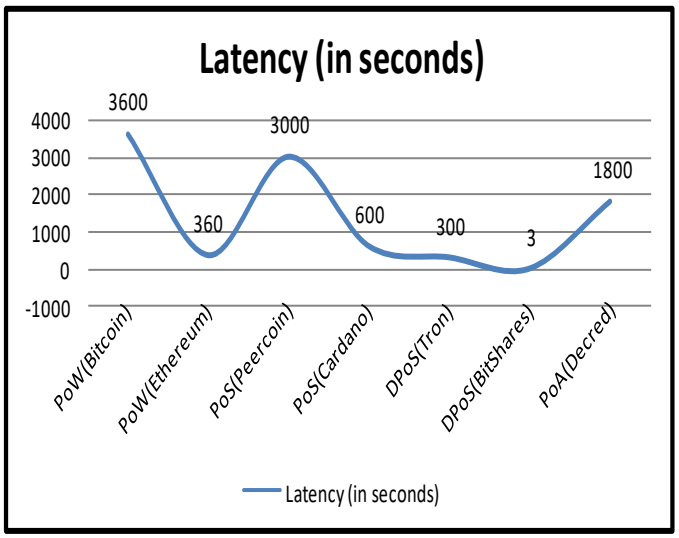


**FIGURE 8.** Latency in seconds for different consensus protocols implementations.

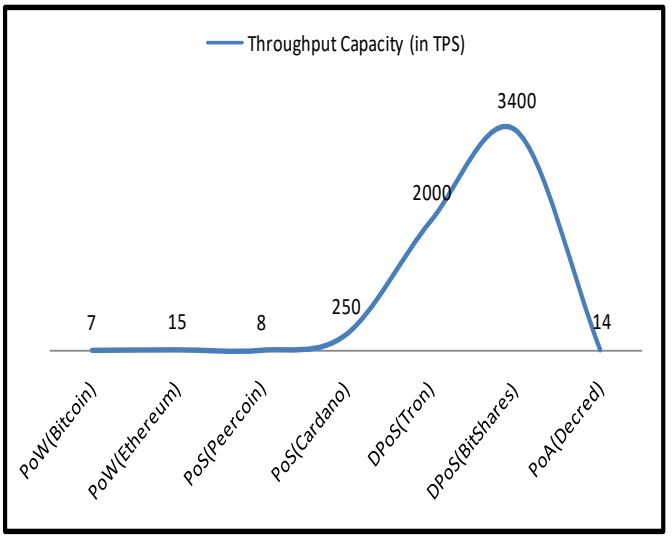


**FIGURE 9.** Throughput capacity (in TPS) of consensus protocols.

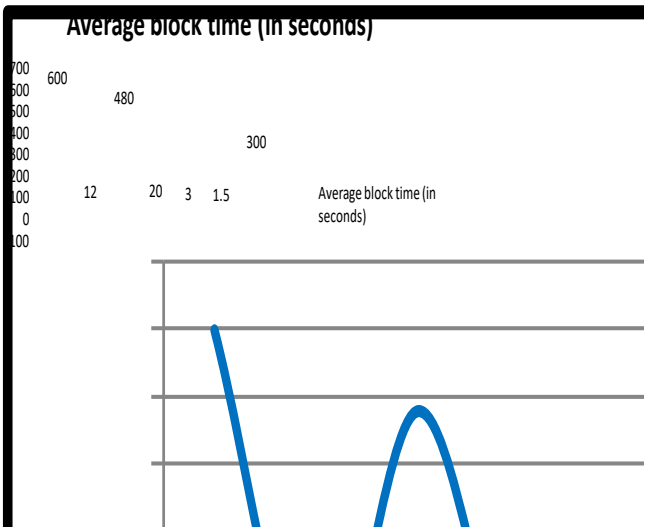


**FIGURE 10.** Average block time in seconds for consensus protocols.

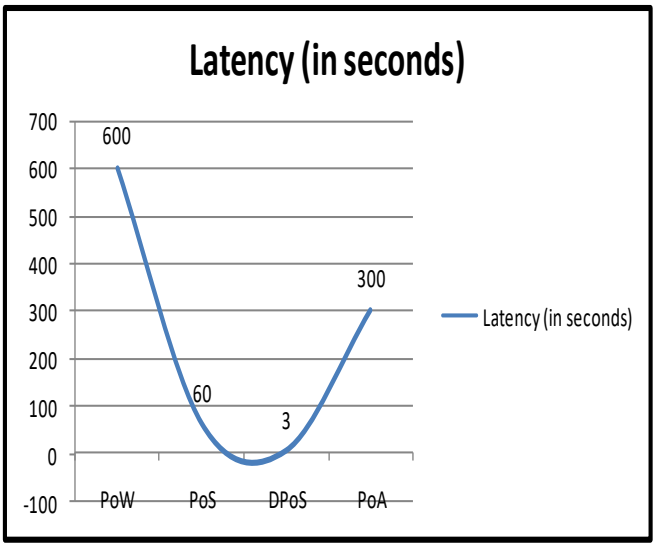


**FIGURE 11.** Latency of different consensus protocols.

- Fault Tolerance Rate: It is measured as to how the ledger's validity and throughput vary when some nodes fail. The rate of fault tolerance in case of PoW and PoS is 0.49 and 10/21 i.e. 0.47 in case of DPoS. We do not have any statistical for PoA. It solely depends upon the smart contract designed for the application. If a node running the smart contract fails, the entire blockchain application will compromised. Therefore, to make the system more tolerant to such crashes the smart contracts are replicated over number of nodes.
- Adversary Tolerance: It represents the percentage of the Blockchain network that, without affecting consensus, could tolerate failure or attack. It is based on the assumption that PoW is affected by number of attacks thus adversary tolerance is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3085187, IEEE Access



found to be less than 25% of the total computational power of the system in case of Bitcoin and Ethereum both. The PoS is adversary tolerant is found to be dependent upon the algorithm and it should be ≈50% stake. In DPoS and PoA it has been remained the same as ≈50%.

PoA.

- Security: PoW is more susceptible to 51 % attack, whereas PoS and DPoS have reduced the vulnerability of 51% attack to some limit and PoA has eliminated its probability of occurrence.
- Overhead: It represents the additional expense in terms of computing resources, network surcharges, and storage space required for each block created.
- Scalability: Due to the growing number of computation nodes, latency and throughput changes can be termed scalability. PoW has poor scalability due to less TPS, whereas it is considerably fair in PoS and limited in DPoS and PoA.

Hence all these parameters are compared and analyzed. Due to the stability, latency and throughput issues there is always a scope of hybridization of these protocols to provide improved and efficient consensus protocol version.

TABLE II
PERFORMANCE COMPARISON OF VARIOUS CONSENSUS ALGORITHMS [1, 28, 33, 34, 38]

| | **PoW** | **PoS** | **DPoS** | **PoA** |
|---|---|---|---|---|
| Applicability | Public | Public | Public | Permissioned |
| Basis of assigning accounting rights | Computing Power | Stake | Stake votes | Activity based |
| Degree of decentralization | High | High | Medium | Low |
| Accounting nodes | Whole network | Whole network | Selected nodes | Selected nodes |
| Latency (Response Time) | 10 min | 1 min | 3 s | 5 min |
| Throughput capacity (TPS) | ≥ 7 TPS | ≥300 TPS | ≥500 TPS | ≥14 TPS |
| Fault tolerance Rate | 49% | 49% | 10/21 | Unknown |
| Adversary Tolerance | < 25% computing power | < 51% Stakes(depends on specific algorithm used) | < 51% delegators | < 51% online stake |
| Computing Overhead | High | Medium | Medium | High |
| Network Overhead | Low | Low | N/A | Low |
| Storage Overhead | High | High | High | High |
| Scalability | Not scalable | Scalable | Partially Scalable | Partially Scalable |
| Security | Attacks are possible with 51 percent hash power, which in the real world is impractical. | Less prone to 51 percent attack as compared to PoW. | Less vulnerable to 51% attack than PoW and Strong protection against double spending. | Removes 51 percent attack threat |
| Mining Rewards | Mining Fee and Transaction Fee | Amount of coins stacked + Transaction Fee | Transaction fee to be distributed among stakeholder and | Transaction fee to be distributed among active stakeholders |

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3085187, IEEE Access



| | | | | |
|---|---|---|---|---|
| | | | block creator. | and block creator. |
| Typical Application | Bitcoin , Ethereum | Cardano, Peercoin | BitShares, Tron | Decred |
| References | [1,28,33,38] | [1,28,33, 34,38] | [1,28,33.38] | [28,33] |

## VII. CONCLUSIONS AND FUTURE SCOPE

Blockchain technology is emerging to be the most disruptive innovation in this decade. Its characteristics of decentralization and strict encryption have lead to blockchain being considered as protected technology. A detailed knowledge of blockchain architecture, various blockchain consensus algorithms can lead to well informed decisions and further research in creating a more secure, protected and encrypted scalable blockchain technology. The research has focused mainly on providing a detailed view of blockchain architecture, the various characteristics of blockchain architecture. As the consensus layer is the core component of performance and security measures of the Blockchain network, therefore, a number of consensus protocols have been introduced to maximize Blockchain systems' efficiency and meet application domains' individual needsfor maintaining transaction reliability and validity. The paper highlights the detailed discussion of main consensus protocols mainly Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Activity (PoA).

In this paper first a literature review of research on blockchain technology presents the overview of the technology and its various characteristics, then a detailed blockchain architecture is presented discussing all the layers viz. Network layer, Consensus Layer, Data model layer , Execution Layer, Application Layer along with the characteristics of layered architecture. The paper mainly focuses on consensus layer highlighting the most common consensus protocols PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated PoS), PoA (Proof of Activity) which act as a tool for maintaining reliability and validity in the architecture. The paper presents the working of all these algorithms either in the form of flow charts or pseudo codes. A summary of various advantages and disadvantages of all these algorithms is summarized in the form of Table I.

The main outcome of the paper is performance analysis framework of these consensus algorithms which is in the form of a performance matrix based on a number of significant parameters which are applicability, basis of assigning accounting rights, degree of decentralization, accounting nodes, latency, throughput, fault tolerance rate, adversary tolerance, overhead, scalability, average block time as presented in Table II.

The comparison for some important parameters are illustrated further with the help of graphical representations, for example throughput is maximum for DPOS protocol and Average block time and Latency is maximum in POW. However, PoA is best among all four to reduce the 51% attack.

As future work, the paper provides the highlights of state of art consensus protocols mainly Proof of work (PoW), Proof of stake (PoS), Delegated proof of stake (DPoS), Proof of activity (PoA) and provides a comparative analysis of these protocols on the basis of significant parameters. As blockchain is one of the major disruptive technologies that can redefine several existing domains of applications and consensus methods is core element for the success of underlying blockchain architecture. The ideal consensus method is yet to explore as almost every consensus mechanism developed have disadvantages and security issues. Therefore, we would like to explore our research further to get a hybrid consensus method that would be reduce the shortcomings of these conventional consensus algorithms and provide a sound consensus mechanism with the desired performance and security concerns. This paper would help researchers to further delve into more detailed analysis based on specific application domains.

## REFERENCES

[1] S. S. Hazari and Q. H. Mahmoud, "Comparative evaluation of consensus mechanisms in cryptocurrencies," *Internet Technol. Lett.*, vol. 2, no. 3, p. e100, 2019.

[2] Hashim, M. (2019) Decrypting Practical AI: Empowering or Enslaving Humans? [Online]. Available: https://www.researchgate.net/publication/332555792_ DECRYPTING _PRACTICAL_AI_EMPOWERING_OR_ENSLAVING_HUMANS. [Accessed: 24-Mar-2021].

[3] C. V. N. U. B. Murthy, M. L. Shri, S. Kadry, and S. Lim, "Blockchain based cloud computing: Architecture and research challenges," *IEEE Access*, vol. 8, pp. 205190–205205, 2020.

[4] S. Nakamoto and W. bitcoin.org, "Bitcoin: A peer-to-peer electronic cash system," *Bitcoin.org*. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: 23-Mar-2021].

[5] T. Neudecker and H. Hartenstein, "Network Layer Aspects of Permissionless Blockchains," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 1, pp. 838–857, 2019.

[6] H. Wang, Y. Wang, Z. Cao, Z. Li, and G. Xiong, "An overview of blockchain security analysis," in *Communications in Computer and Information Science*, Singapore: Springer Singapore, 2019, pp. 55–72.

[7]*Ctfassets.net*. [Online]. Available: https://assets.ctfassets.net/sdlntm3tthp6/6bcDZ5ubSweak68KkUCoA A/41fe3f129eb373 a7107e295c70f3de52/A-Gentle-Introduction-To-Bitcoin-WEB.pdf. [Accessed: 23-Mar-2021].

[8] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, 2016.

[9] P. Javeri, "Blockchain Architecture - prashun javeri - Medium," *Medium*, 13-Jan-2019. [Online]. Available: https://medium.com/@prashunjaveri/blockchain-architecture-3f9f1c6dac5e. [Accessed: 23-Mar-2021].

[10] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "BLOCKBENCH: A framework for analyzing private blockchains,"

in *Proceedings of the 2017 ACM International Conference on Management of Data - SIGMOD '17*, 2017.

[11] Dib, Omar & Brousmiche, Kei-Léo & Durand, Antoine & Thea, Eric & Hamida, Elyes, "Consortium Blockchains: Overview, Applications and Challenges," *International Journal On Advances in Telecommunications*, IARIA, 2018, pp. 51-64

[12] Ismail and Materwala, "Article A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions," *Symmetry (Basel)*, vol. 11, no. 10, p. 1198, 2019.

[13] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *Int. j. web grid serv.*, vol. 14, no. 4, p. 352, 2018.

[14] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Advances in Cryptology — CRYPTO' 92*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 139–147.

[15] S. Zhang and J.-H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Express*, vol. 6, no. 2, pp. 93–97, 2020.

[16] S. Wan, M. Li, G. Liu, and C. Wang, "Recent advances in consensus protocols for blockchain: a survey," Wirel. netw., vol. 26, no. 8, pp. 5579–5593, 2020.

[17] S. Leonardos, D. Reijsbergen, and G. Piliouras, "PREStO: A systematic framework for blockchain consensus protocols," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1028–1044, 2020.

[18] H. D. Zubaydi, Y.-W. Chong, K. Ko, S. M. Hanshi, and S. Karuppayah, "A review on the role of blockchain technology in the healthcare domain," *Electronics (Basel)*, vol. 8, no. 6, p. 679, 2019.

[19] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," IEEE Commun. Surv. Tutor., vol. 22, no. 2, pp. 1432–1465, 2020.

[20] S. King and S. Nadal, "PPCoin: Peer-to-peer crypto-currency with proof-of-stake," Decred.org. [Online]. Available: https://decred.org/research/king2012.pdf. [Accessed: 23-Mar-2021].

[21] "Nxt Whitepaper - Introduction: Nxt Whitepaper," *Nxtwiki.org*. [Online]. Available: http://nxtwiki.org/wiki/Whitepaper:Nxt. [Accessed: 23-Mar-2021].

[22] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment," Comput. Commun., vol. 153, pp. 229–249, 2020.

[23] J. Debus, "Consensus Methods in Blockchain Systems," *Explore-ip.com*. [Online]. Available: http://www.explore-ip.com/2017_Consensus-Methods-in-Blockchain-Systems.pdf. [Accessed: 23-Mar-2021].

[24] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 4, pp. 3416–3452, 2018.

[25] M. Finck, "Smart contracts as a form of solely automated processing under the GDPR," *Int. Data Priv. Law*, vol. 9, no. 2, pp. 78–94, 2019.

[26] A. Deshpande et al., ''Distributed ledger technologies/blockchain: Challenges, opportunities and the prospects for standards,'' British Standards Inst., London, U.K., Tech. Rep., 2017. [Online]. Available: https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_D LT_Web.pdf. [Accessed: 23-Mar-2021].

[27] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted Execution Environment: What It is, and What It is Not," In Proceedings of the *2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, 20–22 August 2015; Volume 1,pp. 57–64.

[28] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism," *IEEE Access*, vol. 7, pp. 118541–118555, 2019.

[29] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain Consensus Algorithms: A Survey," arXiv [cs.DC], 2020.

[30] G. Hardin, "The tragedy of the commons," *Science*, vol. 162, no. 3859, pp. 1243–1248, 1968.

[31] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]y," *Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, 2014.

[32] "Decred - Secure. Adaptable. Sustainable," *Decred.org*. [Online]. Available: https://www.decred.org. [Accessed: 23-Mar-2021].

[33] F. Y. Wang *et al.*, "Study of blockchains's consensus mechanism based on credit", *IEEE Access*, vol. 7, pp. 10224-10231, 2019.

[34] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Syst. Appl.*, vol. 154, no. 113385, p. 113385, 2020.

[35] J. H. Mosakheil, "Security Threats Classification in Blockchains," St. Cloud State University, 2018.

[36] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telemat. inform.*, vol. 36, pp. 55–81, 2019.

[37] M. Salimitari and M. Chatterjee, "A survey on consensus protocols in blockchain for IoT networks," *arXiv [cs.NI]*, 2018.

[38] A. H. Alkhazaali and O. Ata, "Lightweight fog based solution for privacy-preserving in IoT using blockchain," in *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2020.

[39] R. Zhang, R. Xue, and L. Liu, "Security and Privacy on Blockchain," *arXiv [cs.CR]*, 2019.

[40] C. Lepore, M. Ceria, A. Visconti, U. P. Rao, K. A. Shah, and L. Zanolini, "A survey on blockchain consensus with a performance comparison of PoW, PoS and Pure PoS," *Mathematics*, vol. 8, no. 10, p. 1782, 2020.

[41] Feng, Q., He, D., Zeadally, S., Khan, M., & Kumar, N. (2019). A survey on privacy protection in blockchain system. J. Netw. Comput. Appl., 126, 45-58.

[42] A Suresh, A R Nair, A Lal, M Kumaran S, G Sarath. (2020, July). A Hybrid Proof based Consensus Algorithm for Permission less Blockchain. Second International Conference on Inventive Research in Computing Applications (ICIRCA), 707–713.

[43] Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & Security, 97(101966), 101966.

[44] Wang, E. K., Liang, Z., Chen, C.-M., Kumari, S., & Khan, M. K. (2020). PoRX: A reputation incentive scheme for blockchain consensus of IIoT. Future Generations Computer Systems: FGCS, 102, 140–151.

[45] Qadir FutuQ. M., Rashid T. A., Al-Salihi N. K., Ismael B., Kist A. A., & Zhang Z. (2018), Low Power Wide Area Networks: A Survey of Enabling Technologies, Applications and Interoperability Needs, *IEEE Access*, 6, 77454-77473, doi: 10.1109/ACCESS.2018.2883151.re

[46] Ajay K, Kumar A., Bharat B., & Chinmay C. (2021), Secure Access Control for Manufacturing Sector with Application of Ethereum Blockchain, Peer-to-Peer Networking and Applications, 1-17, https://doi.org/10.1007/s12083-021-01108-3

[47] Godar J. Ibrahim, Tarik A. Rashid, Mobayode O. & Akinsolu (2020), An energy efficient service composition mechanism using a hybrid meta-heuristic algorithm in a mobile cloud environment, Journal of Parallel and Distributed Computing, 143, 77-87, https://doi.org/10.1016/j.jpdc.2020.05.002.

[48] Chinmay C., Pathak S.S., & Chakrabarti S. (2009), An O(n) Telephony Gateway Selection Methodology for IP-PSTN Packet Routing, IEEE INDICON, 517-520.

[49] Amit K., Chinmay C., & Wilson J. (2021), Reinforcement Learning for Medical Information Processing over Heterogeneous Networks, Springer Multimedia Tools and Appl, https://doi.org/10.1007/s11042-021-10840-0

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3085187, IEEE Access



**Manpreet Kaur** received the B.Tech. degree in computer science and engineering from Punjab Technical University, Punjab, India in 2007 and her M.Tech. degree from College of Agricultural Engineering and Technology, Punjab Agriculture University, Ludhiana in 2010. She is currently an Assistant Professor with the Guru Nanak Dev Engineering College, Ludhiana. She has been engaged in teaching and research in the field of Software Engineering. Her research interests include the opinion mining, blockchain technology and its consensus mechanism, artificial intelligence. She has published 03 international journal papers and 01 international conference paper along with 01 chapter in a book. She is also pursuing her Ph.D degree from Chandigarh University, Gharaun in the area of blockchain technologies.

Mohammad Zubaire Khan received the M.Tech. degree in computer science and engineering from U. P. Technical University, Lucknow, India, and the Ph.D. degree in computer science and information technology from the Faculty of Engineering, M. J. P. Rohilkh and Univer- sity, Bareilly, India. He was the Head and an Associate Professor with the Department of Computer Science and Engineering, InvertisUniversity, Bareilly. He is currently an Associate Professor with the Department of Computer Science, College of Computer Science and Engineering, Taibah University. He has published more than 60 journals and conference articles. He has more than 15 years of teaching and research experience. His current research interests include the IoT, machine learning, parallel and distributed computing, and computer networks. He has been a member of the Computer Society of India since 2004.

Shikha Gupta is an Academician and researcher with vast academic experience in Institutes of repute. Presently she is associated with Chandigarh University as associate professor in University Institute of Engineering (Computer Science). Her area of interest are Data Analytics, Artificial Intelligence, Data mining, blockchain technology, Machine Learning, Deep Learning, Algorithm development and analysis.

Abdulfattah Noorwali (Member,IEEE) received the Ph.D. degree in electrical and computer engineering from the University of West- ern Ontario, London, ON, Canada, in 2017. The title of his thesis was Modeling and Analysis of Smart Grids for Critical Data Communication. He is currently the Chairman of the Electrical and Computer Engineering Department,Faculty of Engineering and Islamic Architecture, UmmAl-Qura University,where he is also an Assistance Professor. He is also a Senior Consultant with Umm Al-Qura Consultancy Oasis, Institute of Consulting Research and Studies (ICRS), Umm Al-Qura University, where he is also the Chairman of Vision office of consultancy. He has authored many technical articles in journals and international conferences. His research interests include smartgrid communications, cooperative communications, wireless networks, the Internet of Things, crowd management applications, and smart city solutions.

Chinmay Chakraborty is currently an Assistant Professor (Sr.) with the Department of Electronics and Communication Engineering, Birla Institute of Technology at Mesra, India. He has published 100 articles at reputed international journals, conferences, book chapters, and books. His current research interests include the Internet of Medical Things, wireless body area networks, wireless networks, telemedicine, m-health/e-health, and medical imaging. He received a Best Session Runner-up Award, Young Research Excellence Award, Global Peer Review Award, Young Faculty Award, and Outstanding Researcher Award.

Subhendu Kumar Pani received the Ph.D. degree fromUtkal University, Odisha, India, in 2013. He is currentlyworking as Principal at Krupajal Computer Academy (KCA), Bhubaneswar. He has published 51 International Journal arti- cles (25 Scopus index). His professional activities include roles as Book Series Editor (CRC Press, Apple Academic Press, and Wiley-Scrivener), associate editor, editorial board member, and/or a reviewer of various International Journals. He is an associate with number of conference societies. He has more than 150 international publications, five authored books,15 edited and upcoming books; 20 book chapters into his account. His research interests include data mining, bigdata analysis, web data analytics, fuzzy decision making, and computational intelligence. He is a Fellow in SSARS Canda Life Member in IE,ISTE,ISCA,OBA.OMS,SMIACSIT, SMUACEE, and CSI. He was a recipient of five researcher awards.