# Performance Analysis of Blockchain Consensus Protocols- A Review

**Amina Yaqoob Alma Shamas Jawad Ibrahim**
Aminayaqoob9@gmail.com arfa.noor91@gmail.com jawwad.ibrahim@cs.uol. edu.pk
Department of Computer Science and Information Technology, University of Lahore, Gujrat Campus, Pakistan;
Department of Computer Science and Information Technology, University of Lahore, Gujrat Campus, Pakistan;
Department of Computer Science and Information Technology, University of Lahore, Gujrat Campus, Pakistan;

**Abstract**
Blockchain system brought innovation in the area of accounting, credit monitoring and trade secrets. Consensus algorithm that considered the central component of blockchain, significantly influences performance and security of blockchain system. In this paper we presented four consensus protocols specifically as Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) and Practical Byzantine Fault-Tolerance (PBFT), we also reviewed different security threats that affect the performance of Consensus Protocols and precisely enlist their counter measures. Further we evaluated the performance of these Consensus Protocols in tabular form based on different parameters. At the end we discussed a comprehensive comparison of Consensus protocols in terms of Throughput, Latency and Scalability. We presume that our results can be beneficial to blockchain system and token economists, practitioners and researchers.

***Keywords:***
*Blockchain, Consensus Protocols, Security, Performance Measures*

## 1. Introduction

Blockchain is the Bitcoin Revolution infrastructure. Bitcoin is a cryptographic money that guarantees trust and security by means of the execution of projects for the checking and approving exchanges. Blockchain[1] allows digital currency transfers between individuals, without the need for a Bitcoin network central bank or intermediary. It simply incorporates encryption, distributed system technology, peer-to-peer networking and other popular technologies. In addition, blockchain is secure Cryptocurrencies system under which nobody may manipulate transaction material and all nodes can participate anonymously in trades. This is why this technology can be used in different areas such as the banking sector, the medical services, the supply chain and the Internet of Things (IoT)[2]. Blockchain is a distributed ledger containing interconnected blocks and block hash. It records data blocks that have been initiated in the Blockchain Network by participating notes. Block is the fundamental unit of Blockchain, which combine block header and block data.

The Block header usually including current Block Hash, root Hash, time stamp, Nonce and previous Block whereas the data portion of block contains the total transaction number (Sender address, transfer value, address of recipient, transaction cost, etc.). In Blockchain, blocks are connected together with Merkle tree, acyclic directed graph etc. and can be recovered by means of an underline protocol scheme

It can be classified as below based on the need to receive authorization in Blockchain: permissioned and permission less blockchain. In permissioned blockchain, permission is required to enter this form of Blockchain. Only approved parties can execute nodes in the Blockchain network to verify transactions. Whereas to participate in permission less Blockchain, no prior authorization is needed. Everyone is permitted to take part in the authentication process and have their own computational power in the Blockchain network.

A third category of blockchain is Hybrid blockchain, there may be a chance that a node participates in Permission less and permissioned Blockchain together, which can be considered Hybrid Blockchain for inter-Blockchain contact. You may also customize a Blockchain network to support permission-free or permission models. Blockchain has three types: public, fully private and consortium blockchain. In public blockchain, there is no authority or no party with more influence. Everybody here is open to go or to enter. The blockchain has the right to verify a transaction online.

In consortium blockchain not[3] everyone has the same right to validate transactions, A few citizens are privileged to validate the transactions. The fully private blockchain is a very different implementation of this kind of blockchain. The system is centralized. A single body can take decisions and even controls the validation process. The central head ensures that the following

Manuscript received June 5, 2023
Manuscript revised June 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.6.23

consensus is the one it proposes. The public blockchain scheme is also classified as permission less blockchain whilst the other two groups fall under the permissioned. The permitted blockchains are quicker, more energy efficient and easier to execute than the permission less blockchains.

This paper divided into various sections; section 2 provides the need for consensus protocols. Section 3 include main consensus protocols, section 4 illustrates the security issues and challenges to blockchain, section 5 defines performance analysis of consensus protocols, section 6 demonstrates performance evaluation and discussion using three parameters and finally section 7 includes conclusion of the paper.

## 2. NEED FOR CONSENSUS PROTOCOLS:

The world has been revolutionized by distributed ledger technology, turning traditional processes into more stable, reliable and scalable. The framework offers a trustworthy repository between a groups of nodes in a network that does not trust each other completely. There have been several successful implementation versions of this system since the emergence of Bitcoin in 2008, including Ethereum, Hyperledger, Tangle, Corda, etc. All these versions vary in how they agree, which allows a distributed directory to operate equally, reliably and effectively.

A consensus protocol, the central part of the distributed ledger, performs two tasks; it ensures that the next network block is the only version of the reality, and it safeguards the network against adverse node and network influences[4]. Consensus, literally, means agreement. Consensus algorithms are algorithms that make decisions unanimously by a hierarchical or decentralized network any time needed. It helps the network to validate the transactions without relying on the central authority of the intermediary. A consensus protocol makes a ledger functional and the protocol defects is the ledger's responsibility. Therefore, the researchers and industry have a strong interest in it [4]. There are many types of consensus protocols but proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT) will be discussed here.

## 3. Overview of Consensus Protocols

### 3.1 Proof of work (Pow):

Proof of work (PoW)[5] is a system for agreement inside a blockchain network which is the basic consensus paradigm for different Cryptocurrencies like Bitcoin and Ethereum. The process of PoW is focus on a puzzle resolution. Nodes compete to build up next block
To construct the next block a node has to:

- Check the transactions which are part of block
- Build header

The header of the block consists of various elements:

- the root of Merkle tree's (recall that the transactions are stored in the form of a Merkle tree in the core of the block; as for the block header, it will only store the root of that data structure)
- The previous block hash (relate the block to the previous block, thereby forming a block chain)
- Restriction on the puzzle solution
- Timestamp
- Nonce

Once the miner finds the nonce, i.e. when the miner lifts the puzzle. The node is sent to the other nodes of the network until the block has finalized. The nodes check that the block is correctly generated and link it to the block chain to validate its relation to the history of the transaction [6].The flow of Pow is shown below:

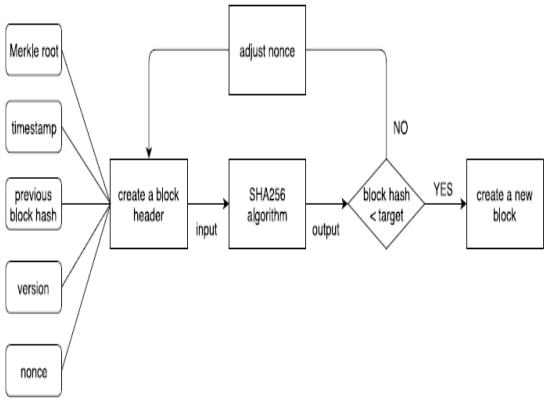



**Fig1:** flow of Pow

A PoW puzzle will quite hardly be solved. Nodes must continue to change their value to get the right answer, which takes a lot of computational power. The malicious attacker will overthrow one block in a chain. However, as the valid blocks of the chain rise, workload

is often accumulated and thus a large amount of computing power is required to overthrow a long chain. PoW is one of the consensus protocols for probabilistic purposes because it ensures a possible continuity .

### 3.2 Proof of Stake (PoS):

PoS which is more energy consuming, is the alternative to PoW. The goal of both being equal, i.e. to find a consensus in the blockchain, but method to achieve the goal is totally different. It uses a selection mechanism which is pseudorandom in nature to choose the validator from existing nodes of the corresponding block. The mechanism is dependent on a combination of various variables, including randomization and staking age of the node's wealth. Blocks are claimed to be "forged" in PoS[7] mechanism, rather than mined. While the block that solves difficult problems and mine the blocks first in PoW, is rewarded. The node that generates the next block in PoS is chosen according to how much you "staked" in relation to other nodes. Currently the stake is dependent on the amount of coins that the network node is trying to mine for that particular blockchain. The transaction fee is usually rewarded in these schemes and consumers who want to be a part of the forging mechanism have to lock their stakes (some coins) on a network. The probability of a node being chosen as the validator varies according to their stake size and, as their stake grows, the chances of a node winning the next block rise. However, these selection parameters are biased because the single node with the highest stake dominates the network. In order to solve this problem, the selection process includes more methods: two of which are "randomized selection of blocks" and "coin-age selection".

**Randomized block selection:** The next forger is chosen based on a combination of hash value and stake in the randomized block selection process, and the node with the maximum stake and the lowest hash value is selected. But the nodes will predict the next forger in this situation, since the stake's size is public by network nodes.

**Coin age selection:** The next forger is chosen based on the time the stake is maintained along with the size of the stake, which is referred to as the age of coin. It is determined by multiplying the number of coins stacked by the number of days they have been held at stake. If the node forges a block, the coin age is set to zero again. And in order to avoid the blockchain being dominated by big stake nodes, the node must wait before another block is created, after building a block [8]. POS is an energy-efficient protocol that uses a way to encourage internal currencies rather than consuming much computational power. Like PoW, PoS is also a consensus protocol for probabilistic finality. The first crypto-currency add to PoS to the blockchain was PPcoin [3].

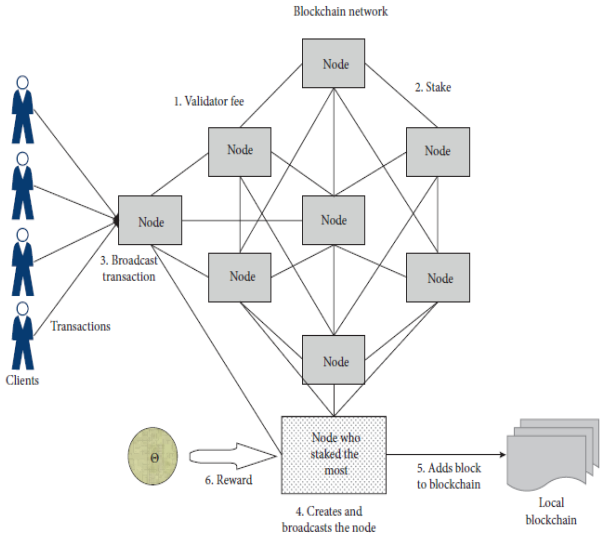



**Fig 2.** Flow of PoS

### 3.3 DPoS (Delegated Proof of Stake):

To speed up the transaction further and resolve the protection issue that the offline node in the PoS should build up the coin age as well. In April 2014, Daniel Larimer suggested DPoS (Delegated Proof of Stake) which is now a consensus system for BitShares and Crypti networks. In DPoS the system presents two roles, which have many participants, known as a witness and delegate [9]. The DPoS consensus process is divided into the initial election of witnesses (i.e. block producers) and subsequent block generation. The witnesses are exclusively responsible for the transaction, verification of the signature and the times tamping, but do not take part in the trade. They create one block every 3s and will be overwritten and replaced by the next if a witness has not completed the task at a specified time. The participants are chosen according to the numbers of stakeholders in the approval voting process. Stakeholders with a stake of more than 51% will vote for N witnesses and delegates. The more blockchain stakes it has, the greater his possibility of a witness. Each node in the network can vote for its own, trusted witness [8]. The witnesses themselves are unrelated to their participating transaction records. They are only involved in the generation of the block and get transaction fees revenue.

As the joint signers of the account of the stakeholder the delegates must change the process such as the method of creating the witness block and the transaction charges. The modification is carried out under the control of the stakeholders. Compared to the PoS node, each node has the same right to create a block, the DPoS nodes are split into delegates and witnesses with different privileges. The distinction between PoS and DPoS is crucial. Delegates are responsible for voting, and witness are only for their follow-up nodes [8].

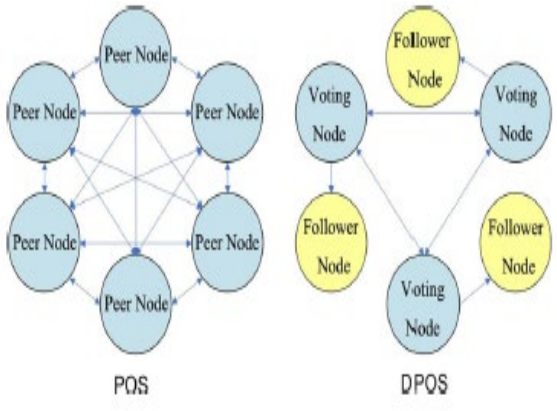



**Fig 3.** Node difference between PoS and DPoS

DPoS is a cost-effective consensus protocol compared with PoW and PoS. DPoS has now been converted from the new edition of EOS to BFT-DPoS [3].

### 3.4 Robust Proof of stake (RPoS):

Three features of PoS consensus protocol include energy-saving, speed of trade, risk of accumulation of coin age and Nothing at Stake-attack. The robustness of PoS is relatively low due to these attacks.

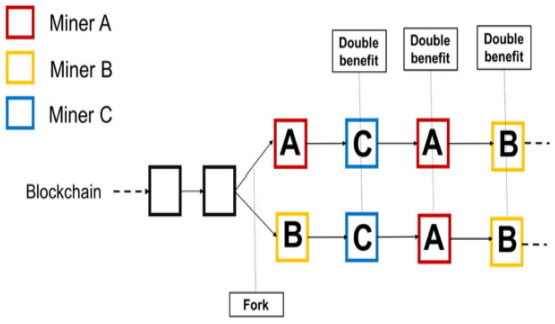



**Fig 4.** nothing at stake attack

In this blockchain architecture, miners have to mine both chains at the same time when nothing at Stake attack happens. Every miner has a motivation to cheat in this case for the double profit. The “Nothing at Stake” attack doesn't lose nothing, but it can gain it all. If the system forks, the malicious node can benefit both chains at no competitive cost. Such attacks frequently occur if the system generates a fork or if it can result from a malicious attack. Furthermore, such attacks are likely to succeed, because everyone in the fork chain has reached a consensus and has not. In response to coinage accumulation problems and “Nothing at Stake” attack Robust Stake Consensus Protocol (RPoS)[10] is constructed. RpoS perform following functions:

**Dynamic coin age:** As there are too many mining nodes, we suggest the notion that acts as a threshold, the 'dynamic coin age. Only the coin age-condition node can compete for the packing opportunity and receive the system reward.

Calculation of coin age: We first measure the time accumulation and number of coins before we calculate the coin age of the node. Each block has a timestamp, and you can get the accumulated time by the timestamp, which is:

$$Age_t = (D_t - D_{t-1}) * N_{coin} + Age_{t-1}$$

Ncoin is a current value in the amount of coins. The new days are the result of the present block time Dt and subtract the previous time Dt-1. The additional days increase the amount of Ncoin and lead to a new coin age. Afterwards we get the coin age Aget by the new coin age plus the previous coin age Aget-1 alternatively1. The coin age Aget of the node will be cleared after the blocks are packaged.

RPoS mining process: The target value definition is a value which is dynamically adapted to the production time of the block and used to identify the value of the block production.

$$Hash\ (Cont_{block}, Var_{nonce}) < Age_t * AV_{target}$$

Varnonce is the nonce variable where the Contblock variable is the block contents. TheAget*gVtarget, a dynamic coin age, is understood as a result of this hash inequality.

Implementation of RPoS: If you are using coin age, coin age risk will be in PoS attack, so we remove the age of coins and use the quantity of coins to pick miners. Difference between other protocols like PoS and PoW is

find and it is estimated that RPoS satisfies the following formula:

$$\text{Hash}\ (\text{Cont}_{\text{block}}, \text{Var}_{\text{nonce}}) < \text{N}_{\text{coin}} * \text{V}_{\text{target}}$$

The node, who having greater Ncoin is more easily packed and can produce blocks. By adding the dynamic adaptation to the V target, and the maximum number of rollbacks, the double advantage of nodes are lessen that cheating on the fork while a "nothing at Stake" attack is occurring. Upgraded nodes are degraded and restored to an un-upgraded condition by a maximum number of rollback, such that all data returns to its previous state after which the fork is removed. A verification of the rollback block can detect the attack on "Nothing at Stake". However, if the number of the rollback is larger than the maximum number, it will not merge the chain. So only "mining" on the original chain may be done by the cheating nodes. If the block is validated, the rollback number is less than the maximum number, then the valid block will be considered, information will be merged and the transaction behavior will proceed. So. "Nothing at Stake" attacks may be resisted effectively by maximum rollback number in RPoS system [10].

## 3.5 Practical Byzantine Fault Tolerance:

It is a consensus mechanism which is model largely to offer Byzantine replication of a machine resilient to malicious system nodes (byzantine failures) that fail or spread incorrectly Information to its peer nodes. The main purpose of such a method of consensus is to prevent a failure of the system by decreasing the impact of the system Compromised nodes on and around the network achieving the correct agreement with honest nodes. This protocol is described to operate well for non-synchronized systems and to offer excellent performance with a decreased duration even if the data is somewhat delayed[11]. The participating nodes act as a follow[12], [13]:

- In this network nodes involved are placed in a PBFT model in a manner in which the leading nodes (primary) and the remainder of this network are called backup one.
- Entire nodes within the frame interact with one another and agree on a system status by a majority amongst honest nodes.
- Nodes speak actively to one other and do not simply have to confirm that messages originate from a certain network node, but also that the messages have not tampered with in the transmission. In this protocol each round is separated in 4 sections:

1. The pioneer node (leader) is sent to a request for an assistance action by the client node.
2. The Pioneer node multicasted the request for backup nodes.
3. The remaining node requests are then processed and the customer receives a reply.
4. Then, clients predict that the number of nodes which might be broken will be f +1 (f, the extreme number), with a proportionate consequence, from different nodes.

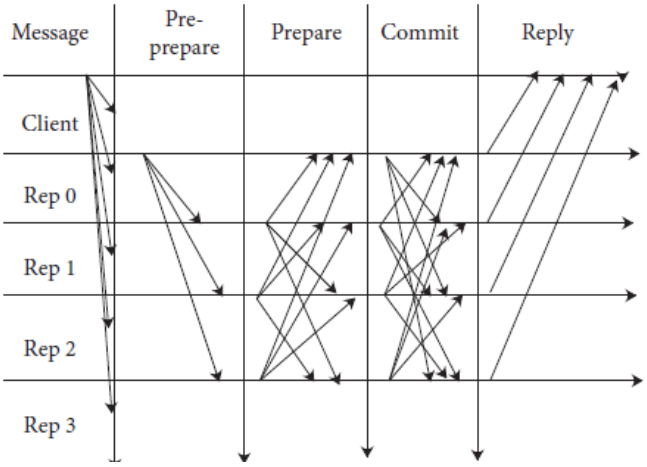



**Fig 4**. Flow diagram of each round

**Table 1. Comparison of blockchain Consensus Protocols**[14]

| | PoW | PoS | RPoS | DPoS | PBFT |
|---|---|---|---|---|---|
| Merits | Get consensus fast, exclude phishing probability and also is verified many times. | It performs better than other protocols in terms of minimum energy consumption, efficient staking and provide friendly environment | By using number of coins instead of age of coins to lessen the threat of attacks occur in existing PoS protocols. | It provides concurrent voting, good reward allocation and provides scalability | PBFT offers transaction validation, energy efficient, minimal payouts are the benefits of PBFT |
| Demerits | Consumption of energy is high to solve complicated math's problem e.g.puzzles | Since it does not need significant computations, hence an attacker can simulate any portion of the blockchain and alternate the blockchain | As in future since system lies on simulation results, so the nodes that define the strength and durability of the system not decided | Producers of block when cooperate introduces other numerous attacks such as double spend and poor voter head count can be exploited | In PBFT nodes identities are private, work for a small number of groups |
| Limitations | More energy used and lost during mining procedure<br><br>Reliance on hardware can result towards the centralization mining | One fundamental drawback is that the network is overtaken by large decision makers | One limitation of the protocol is trade efficiency ratio in terms of scale free network is low than POW and POS. | Organize delegates in small number of cartels makes it less decentralized | If the main nodes(primary) do not work then it is necessary to implement on all over the network and hence reduced efficiency |
| Security Threats | PoW vulnerable to selfish mining, in addition to 51% attack and eclipse attack | PoS is vulnerable to Revisions and double spend attack as the cost and energy demand to modify chain is not feasible.<br><br>Coin age Accumulation and Nothing@Stake attack | Alleviate Coin Accumulation and Nothing@Stake attack faced by existing PoS | It decreases decentralization as rule of making decision relatively confined to few people, organizing a "51%" attack is easier. Bribing and<br><br>DDoS attack | Insecure against Syble Attack |
| Applications | Bitcoin, Litecoin, Ethereum | Peercoin, Ethereum 2.0, Nxt, | Peercoin, Ethereum,Blackcoin | BitShares | Zilliqa , Hyperledger fabric, |

## 4. Security issues and challenges to blockchain:

In this paper we review different security threats and challenges[15], [16] faced by different consensus attacks in order to provide security and reliability in blockchain technology for efficient transfer of data blocks in blockchain. Different types of attack on protocols and their countermeasures are listed below:

**Table 2. Consensus Protocols' Attacks and Countermeasures [10], [14]**

| Attack | Description | Protocol | Countermeasure |
|---|---|---|---|
| 51% Attack | In this attack a group is able to focus the bulk of the network hash rate, obtain the ability to fraudulently verify and control transactions. | PoW | crypto-coin with low hashing power |
| Selfish Mining Attack | A mining node keeps its blocks hidden and distributes them gradually instead of releasing the created block once added to the blockchain | PoW | Truth state |
| Eclipse Attack | malicious attacker establishes all connections possible with the target node | PoW | use whitelists, disabling incoming connections |
| Sybil Attack | Ruins the computer safety reputation system by faking an ID in network | PoW | Monitoring the nodes' behavior<br>Checking the nodes who forward block only for one user |
| Nothing-At Stake Attack | Generate conflicting blocks on all feasible forks in order to maximize earnings via nothing at stake | PoS | Three strikes<br>auxiliary output |
| Grinding Attacks | computational resources may be utilized to influence opposition parties' leading elections | PoS | Entropy based chain into target hash calculation |
| Double Spending Attack | A potential flaw in digital cash is presented, as the same digital token which can be use twice if this attack happens | Not defined | MSP (Multistage Secure Pool) framework that allows the pool to authenticate the transactions. |
| Liveness Attack | Can delay the acknowledgement time of target transaction also delay transaction confirmation time | Not defined | Conflux's consensus protocol essentially follows two strategies:<br>One is the optimal strategy that allows quick confirmation<br>Conservative strategy that guarantees the progress of consensus. |

## 5. Performance Analysis

In this section we precisely analyze the performance of various consensus algorithms, as each consensus protocol has its own efficiencies and drawbacks. In table 3 an analysis of consensus algorithm performed based on the following metrices.[1][17]

**1. Consumption Of Power**: The electricity required for processing the tasks. In PoW more power required to mine a block hash header in order to reach consensus, while Miners in PoS and DPoS make decisions based on the stake (the quantity of coins as well as the age) and low energy usage of PoS. and DPOS. In PBFT no mining power required for consensus process.

**2. Attack's Robustness:** It indicates that the protection against different types of security attacks occur in a blockchain network.

**3. Transaction Per Seconds:** A protocol which instantly validates the transactions and reach

consensus quickly has a higher rate of transaction throughput. PoW algorithm has a low TPS than other protocols because consumes more time to solve puzzle problems.

**4. Identification of nodes:** The identification of each miner must be understood to choose a major in the networks. In case of Pow, POS, DPoS, RPoS identification of nodes related to the network i.e public. PBFT 'node identity is private in order to choose a validator in each round.

**5. Adverse Tolerance:** A system small percentage which can be affected without affecting the consensus. Each model of consensus has an adverse tolerance threshold.

**6. Latency:** Latency refers to as delay or the time it takes a data block to transfer over the medium. It depends upon the block time and number of transactions placed in a block

**7. Consensus finality:** Demonstrates that when a transaction placed in a block it is assumed to verified and cannot be pushed back.

## Table 3. Performance comparison of consensus Protocols

| Metrics | | POW | POS | RPOS | DPOS | PBFT |
|---|---|---|---|---|---|---|
| Consumption Of Power | | Highest | Lower | Lowest | Lower | Lowest |
| Attack's Robustness | 51% Attack | High | Lower | Lowest | Lower | |
| | Coin Age accumulation Attack | N/A | Highest | Lowest | Lower | N/A |
| | Nothing @Stack | N/A | Highest | Lowest | Lower | N/A |
| | Grinding Attack | N/A | Lower | N/A | N/A | N/A |
| Transaction Per Second | | 7 tps | 30-40 tps | ≈40 tps | =>40 tps | 4 times higher than PoW |
| Identification Of Nodes | | Public | Public | Public | Public | Private |
| Tolerated Power Adversary | | >25% computation power | <51% staking problem | Not known | <51% validators | 33.34% incorrect copies |
| Latency | | 6 blocks | 6 blocks | Network Delay | Network Delay | Overall network delay |
| Consensus Finality | | Not guaranteed | Not Guarantee finality | Partial | Partial | Guaranteed |

## 6. Performance Evaluation and Discussion

In this paper we review performance comparison of above defined consensus protocols in terms of different parameters[18]–[20] e.g., throughput, latency and scalability. Throughput defines as number of transactions executed in a given set of time in a blockchain network, it depends on the block size, block interval, that currently involves in a communication over the network. Latency refers to as delay or the time it takes a data block to transfer over the medium. And the final parameter is scalability which means the network's capabilities to expand, the network nodes participating in the consensus or clients, it depends on number of nodes, clients, latency, transaction time.

**Performance analysis of Throughput**

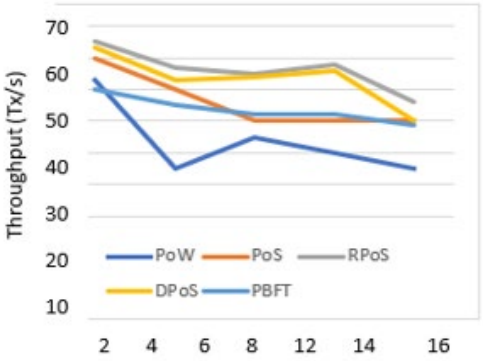



**Fig 1.** Transaction vs. Throughput

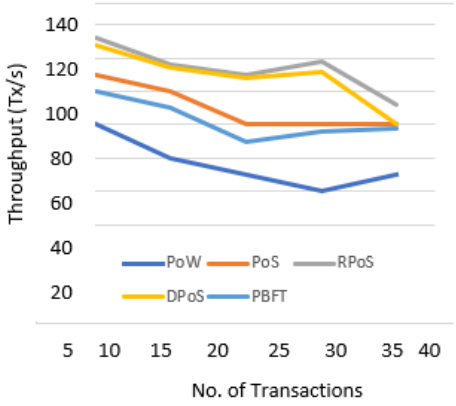



**Fig 2.** Transaction vs. Throughput

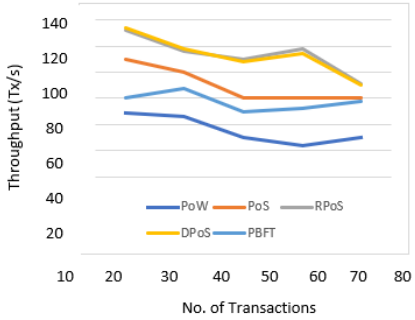



**Fig 3.** Transaction vs. Throughput

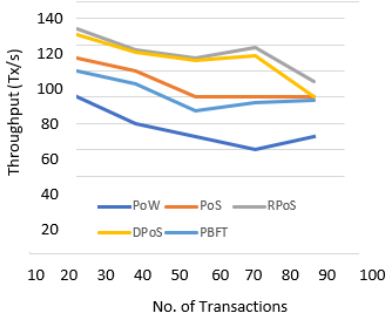



**Fig 4.** Transaction vs. Throughput

Figure.1,2,3 and 4 have shown the affect of throughput in varying the number og transactions. Fig 1 indicates that PoW has a lowest throughput among other consensus protocols because it has limited frequency of block generation which is 7 transaction per seconds and maximum blocks size is 6. After every 10 mins a new block added in blockchain a node must has to wait on average one hour to ensure that the transaction is complete. On the other hand, usually in PoS the size of the block is larger and has a significantly smaller block time i.e.,64s, so the transaction throughput increased significantly that is nearly equal to 875 tx/s. In addition, a number of POS's networks can accomplish their abrupt end, i.e., k = 1, which significantly reduces their confirming time to 1 second. PoS can performs thousands of transactions per second independent of the block size. RPoS and DPoS have almost the highest throughput among all protocols, size of the block in DPOS is large and the block time is significantly short i.e.,3s which increase the transaction throughput. PBFT has throughput higher than PoW, as the transactions increases in between 1 and 100 throughput of both protocols increases, PBFT throughput gain 1024.19 tx/s which is 4.5 times greater than PoW. As the number of transactions increases from 100, throughput of both protocols slightly decreases, PBFT still has the higher throughput than PoW.

**Performance Analysis of Latency**

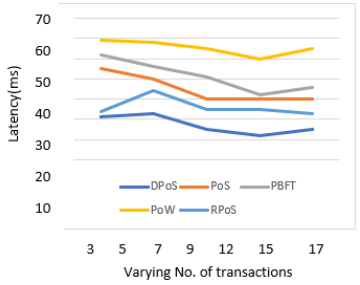



**Fig 5.** Latency vs. transactions

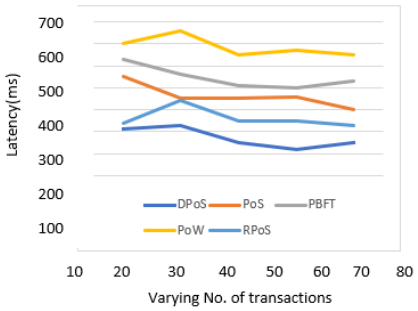



**Fig 7.** Latency vs. Blocks

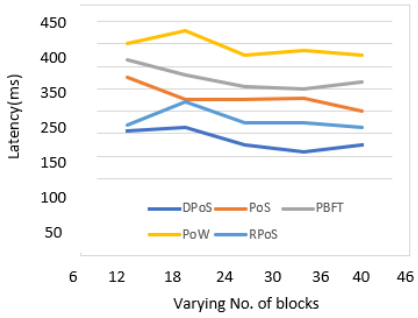



**Fig 6.** Latency vs. transactions

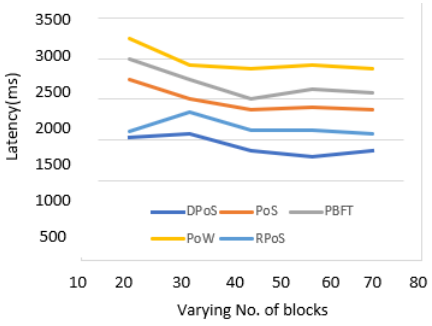



**Fig 8**. Latency vs. Blocks

Fig 5 and fig 6 show the Pow algorithm has the highest latency among other protocols, as the number of transactions increases latency of PoW algorithm increases. Average time rate to create a block in PoW is 10 mins and maximum blocks are 6, so a node requires to wait 1 hour in order to consider a transaction is complete. DPoS and RPoS both protocols have lowest latency because of small block interval i.e. 46s and 13s respectively and varying size of block, so by changing number of transactions and block size would less impact on the latency. PBFT is a private blockchain and works well in small network, though it has small block time i.e., 3s but as the network grows and transaction increasing rapidly the network overhead occur hence latency of the network increases but still less than PoW.

**Performance Analysis of Scalability**[20]

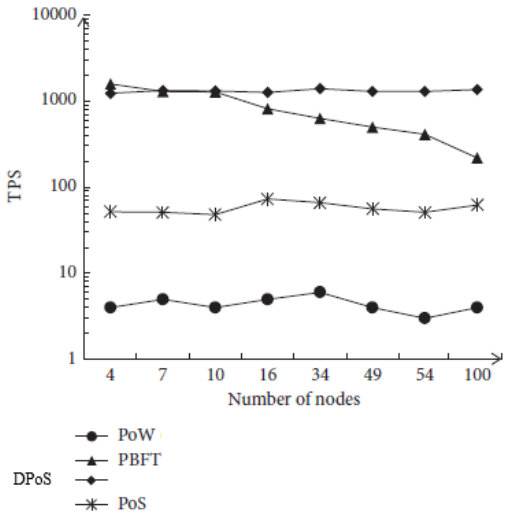



**Fig 9**. TPS vs No. of Nodes

Scalability of an algorithm can be defined as the association between transaction throughput and number of nodes. Fig.9 shows that the scalability of the PBFT drops significantly as nodes grow rapidly. PBFT algorithm TPS values are around 1200 and 218 when four nodes and 100 nodes are present, meaning that under 100 nodes performance is almost 7 times higher than that under 4 nodes. Scalability of PoW, PoS and DPoS are quite steady. The increase in the number of nodes does not have a significant impact on consensus algorithms performance. The PBFT algorithm is concluded[21] to be poorly scalable whereas the 3 other algorithms are highly scalable.

## 6. Conclusion

Block chain technology has already presented its important features in terms of regional autonomy, persistence, privacy and confidentiality and accountability that are morphing manufacturing sectors. This study provides a comprehensive overview of the blockchain, the basic consensus protocols used in blockchain, various types of attacks associated with different consensus protocols are analyzed and their countermeasures to avoid from such attacks reviewed precisely and then these protocols are analyzed and compared using various performance parameters. Neither any consensus algorithm is excellent, and most often there must be some compensation associated with security, performance and efficient scalability are always viewable. Apart of their strengths and weaknesses all of these consensus protocols provide some domain specific alternatives and offer various uses. And at the end, we have a detailed comparison of these protocols in terms of scalability, latency, and Throughput. Performance of All these above protocols depend on different network scenarios under different parameters.

## 7. References


[1] A. Baliga, "Understanding Blockchain Consensus Models," *Whitepaper*, no. April, pp. 1–14, 2017, [Online]. Available: https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf.

[2] B. Mackenzie, B. Mackenzie, X. Bellekens, and R. I. Ferguron, "An assessment of blockchain consensus protocols for the Internet of Things This is the accepted version of a paper presented at the International Conference on Internet of Things , Embedded Systems and Communications ( IINTEC © 2018 IEEE . Personal use of this material is permitted . uses , in any current or future media , including reprinting / An Assessment of Blockchain Consensus Protocols for the Internet of Things," 2018.

[3] A. Altarawneh, F. Sun, R. R. Brooks, O. Hambolu, L. Yu, and A. Skjellum, "Availability analysis of a permissioned blockchain with a lightweight consensus protocol," *Comput. Secur.*, vol. 102, 2021, doi: 10.1016/j.cose.2020.102098.

[4] S. S. Sabry, N. M. Kaittan, and I. M. Ali, "The road to the blockchain technology: Concept and types," *Period. Eng. Nat. Sci.*, vol. 7, no. 4, pp. 1821–1832, 2019, doi: 10.21533/pen.v7i4.935.

[5] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Čapkun, "On the security and performance of Proof of Work blockchains," *Proc. ACM Conf. Comput. Commun. Secur.*, vol. 24-28-October-2016, no. April 2019, pp. 3–16, 2016, doi: 10.1145/2976749.2978341.

[6] A. Porat, A. Pratap, P. Shah, and V. Adkar, "Blockchain Consensus : An analysis of Proof-of-Work and its applications .," pp. 1–6, 2017, [Online]. Available: http://www.scs.stanford.edu/17au-cs244b/labs/projects/porat_pratap_shah_adkar.pdf.

[7] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities," *IEEE Access*, vol. 7, pp. 85727–85745, 2019, doi: 10.1109/ACCESS.2019.2925010.

[8] 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, doi: 10.1109/ACCESS.2019.2935149.

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

[10] A. Li, X. Wei, and Z. He, "Robust proof of stake: A new consensus protocol for sustainable blockchain systems," *Sustain.*, vol. 12, no. 7, pp. 1–15, 2020, doi: 10.3390/su12072824.

[11] W. Mahmood and A. Wahab, "Survey of Consensus Protocols," *SSRN Electron. J.*, no. February, 2020, doi: 10.2139/ssrn.3556482.

[12] "bottleneck of blockchain.pdf." .

[13] Y. Hao, Y. Li, X. Dong, L. Fang, and P. Chen, "Performance Analysis of Consensus Algorithm in Private Blockchain," *IEEE Intell. Veh. Symp. Proc.*, vol. 2018-June, no. Iv, pp. 280–285, 2018, doi: 10.1109/IVS.2018.8500557.

[14] S. Kaur, S. Chaturvedi, A. Sharma, and J. Kar, "A Research Survey on Applications of Consensus Protocols in Blockchain," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/6693731.

[15] N. Chalaemwongwan and W. Kurutach, "State of the art and challenges facing consensus protocols on blockchain," *Int. Conf. Inf. Netw.*, vol. 2018-January, pp. 957–962, 2018, doi: 10.1109/ICOIN.2018.8343266.

[16] N. Chaudhry and M. M. Yousaf, "Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities," *ICOSST 2018 - 2018 Int. Conf. Open Source Syst. Technol. Proc.*, pp. 54–63, 2019, doi: 10.1109/ICOSST.2018.8632190.

[17] L. Ismail and H. Materwala, "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions," *Symmetry (Basel).*, vol. 11, no. 10, 2019, doi: 10.3390/sym11101198.

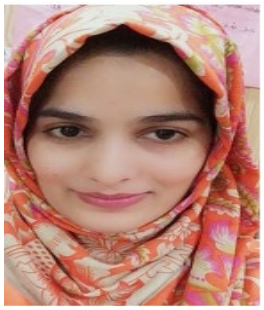
[18] C. Lepore, M. Ceria, A. Visconti, U. P. Rao, K. A. Shah, and L. Zanolini, "A survey on blockchain consensus with a performance comparison of pow, pos and pure pos," *Mathematics*, vol. 8, no. 10, pp. 1–26, 2020, doi: 10.3390/math8101782.

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

[20] Y. Wu, P. Song, and F. Wang, "Hybrid Consensus Algorithm Optimization: A Mathematical Method Based on POS and PBFT and Its Application in Blockchain," *Math. Probl. Eng.*, vol. 2020, 2020, doi: 10.1155/2020/7270624.

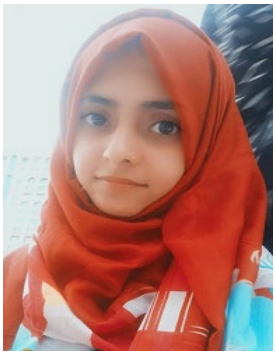
[21] M. Vukolić, T. Quest, B. Fabric, and P. Bft, "The Quest for

Scalable Blockchain Fabric : Proof-of-Work vs . BFT Replication Marko Vukolić To cite this version : HAL Id : hal-01445797 The Quest for Scalable Blockchain Fabric :," 2017.



**Jawwad Ibrahim** received degree in Masters of Sciences in Software Engineering, working as an Associate Professor, Head of Department at Department of Computer Science and Information technology in University of Lahore, Campus Gujrat.

**Amina Yaqoob** Have received BS(IT) degree from University of Gujrat in 2017, working as SSE(CS) in Punjab Education Department, and now doing Computer Science and Information Technology in University of Lahore Pakistan, Gujrat campus. Current research areas and interests are networks, machine learning.



**Alma Shamas** received degree of BS(IT) from University of Gujrat Hafiz Hayat Campus in 2017, after that working as SSE(CS) in Punjab Education Department in Sialkot. Further doing masters in Department of Computer Science and Information technology in University of Lahore Pakistan, Gujrat Campus. Current research areas and interests are networking, programming.