International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Navigating the Blockchain Consensus Landscape: Features, Measured Outcomes and Mitigation Pathways

Sujata Sathe[1], Dr. Sahebrao Shinde[2]

[1]Savitribai Phule Pune University, CMCS College Nasik Centre, India
Email: *sujata.sathe11[at]gmail.com*

[2]Savitribai Phule Pune University, CMCS College Nasik Centre, India
Email: *sns110[at]gmail.com*

Abstract: ***Blockchain technology has evolved incredibly into various domains other than cryptocurrencies such as healthcare, genomics application, agriculture, government schemes, land asset distribution, DeFi, IoT, supply chain management due to its decentralized and secured nature. Consensus mechanism in blockchain networks serves as the backbone to ensure data integrity, provenance, immutability and security. Traditional consensus mechanism faces many challenges like utilization of high energy or carbon, excessive computational resources, staking of cryptocurrency, high reputation of nodes, maximum votes received, scalability and security issues. To tackle this concerns many researchers has proposed solutions and given a comparative analysis of the performance of these algorithms. This paper gives the survey reviews of the consensus mechanism used so far with a comparative analysis on the performance metrics like scalability, latency, and throughput, degree of decentralization, energy and resources efficiency etc. We have divided the consensus algorithms based on two categories i.e Proof based and Acquiescence based. The study highlights critical trade-offs among scalability, energy efficiency, decentralization, fault tolerance, and security resilience. Furthermore, this paper sheds the light on recent innovations addressing mitigation strategies like sharding, off-chain solutions, checkpoint mechanism, and integration of machine learning for anomaly detection, prediction of attack vectors. By systematically comparing consensus protocols and identifying open research challenges, this review aims to provide researchers and practitioners with a clear understanding of current consensus landscapes and provide valuable guidance to the selection and design of suitable mechanisms for next-generation blockchain systems.***

Keywords: Blockchain, Consensus, voting-based consensus, proof-based consensus, BFT-based consensus, sharding.

1. Introduction

A Blockchain is a peer-to-peer decentralized distributed network technology that is immutable, transparent and secured. It is consists of a chain like structure or a ledger composing of a set of transactions encapsulated into a single block that are linked to the previous block using cryptographic hash function. This ledger is append-only ledger, shared and maintained by all the participating nodes of the blockchain network. The first block is termed as the genesis block.

Each node in the network can propose a transaction and broadcasts it for verification to all the other nodes. The node that validates the set of transactions and groups it into the block are miner node which are responsible for block creation and appending it to the existing block. The miner broadcasts the affixing of the new block and other nodes agree upon that. This process is termed as reaching the consensus. Every nodes maintains the same copy after the addition of the new block by the miner. [1]

Blockchains are mainly of four types and fig 1 shows the pictorial representation of blockchain implications depending upon these types of blockchain usage. [2]

a) **Public Blockchain (Permissionless Access):** Anyone can participate in his or her blockchain Network. Bitcoin and Ethereum are its examples
b) **Private Blockchain (Permissioned Access):** Only the verified participants are allowed to join their network.
c) **Consortium Blockchains (Permissioned):** It is also called as Federated Blockchain as it is the combination of Public and Private Blockchain. The blockchain is implemented for various groups of organizations which work in partnership with each other on certain consortium
d) **Hybrid Blockchain (Both Permissionless and Permissioned access):** It is used within the organization for certain groups. It is the combination of public and private blockchain systems. The principal authority controls it with a private permission-based system together with a public system.

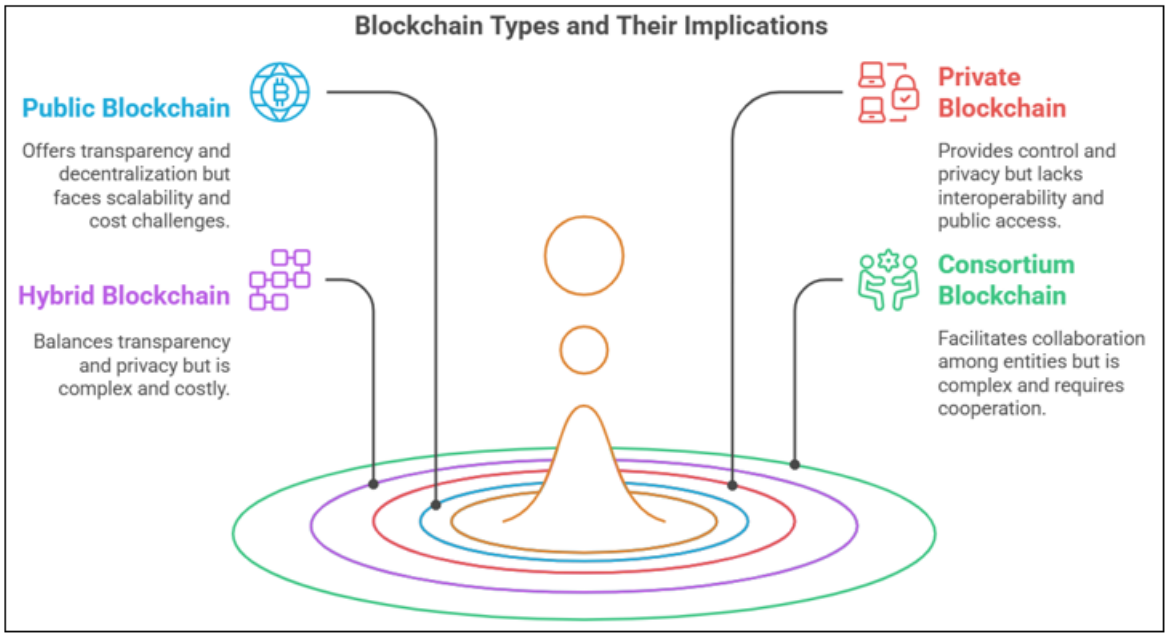


Figure 1: Types of blockchain used for various applications

2. Background

The consensus mechanism are back bone of the blockchain technology are responsible for maintaining the integrity and security of the blockchain. Despite many advancements, current blockchain consensus protocols still face compromises regarding throughput, latency, fault tolerance, security vulnerabilities, and energy efficiency. A consensus algorithm are the protocols that ensures a consistent state of art of the blockchain and agree upon the ordering and sequencing of the transactions. The consensus algorithms are responsible for providing the security and integrity of the state of art of every blockchain. This paper has categorized the consensus algorithms into major two classification, one based on Proofs and other on Acquiesce. The parameters considered for the consensus algorithms are Efficiency, Scalability, Throughput, Latency, Energy-efficient, resource-intensive, incentive/rewards.

Before diving into the actual working principle of each consensus, let us understand the parameters required for consideration of their performance metrics. []

- **Efficiency**: It refers to the fast processing of number of transactions with minimum number of overheads.
- **Scalability**: It refers to the ability of handling increasing number of participants as well as the growing blockchain without comprising the resources and performance of the blockchain
- **Throughput**: It is generally measured in term of TPS i.e transaction processed per second
- **Latency**: It refers to as the delay from submission time of transaction to confirmation time reaching finality.
- **Fault Tolerance**: It is the ability to handle node failures or malicious behaviour without compromising network security.

3. Literature Survey/ Related work

[6] classified the consensus protocol based on two categories:- incentivized and non-incentivized. As the participating nodes compete to add the block, those who are able to solve the mathematical puzzle are considered as the honest nodes and are able to add the new block to the existing chain. The consensus protocol emerging from this process are grouped into incentivized category whereas the protocols where only the authorized (trusted) nodes are allowed to add the new node to the blockchain are grouped into non-incentivized algorithms. The taxonomy of consensus comparison is presented into four major properties Physical Structure, Performance, Reward and Security.

The structural properties of a blockchain network determine how nodes are organized and interconnected to enable their participation in the consensus algorithm.

The reward properties depends on the timestamp of creation of genesis block, incentives provided to the miner for adding the block, total supply of cryptocurrency and average time of block creation.

Security properties of consensus depends on the parameters of throughput (no of transactions processed per time), Scalability (how far the blockchain grows in size and is functional), latency (the delay from the point of the proposing a transaction to its confirmation by consensus.), Attack vectors (resilience to attacks). PoW and PoS are both incentivized algorithms. PoW has limitations of energy and scalability.

[7] The consensus algorithms are analysed and classified into four models namely Competitive, Voting based, Collaborative and other types.

Process of Consensus: The Blockchain network selects a node known as the validator node who wraps up the set of transactions into a candidate block and broadcasts the block to the network.

The other peer nodes verifies the candidate block for authenticity, byzantine fault tolerance and proof of work. Thus, the new block is then added to the local chain of every

node. Therefore, after a certain height of the blockchain is reached and ledger is updated, the new round starts for creation of a candidate block and repeats the same process. The quorum of nodes in a blockchain network performs these rounds.

a) The protocols wherein the nodes are required to compete for computational tasks, resources in order to be accountable for block generation and validations are termed as Competitive consensus mechanism. Proof of Work and Proof of Stake are examples of these mechanisms.
b) The mechanisms wherein the nodes elect their representatives block creation, validation and then addition of newly created block to the chain is termed as collaborative consensus mechanism. These protocols choose their validators depending upon the amount of votes or reputation held by the representative nodes. Delegated proof of work is its example.
c) Voting based consensus mechanism are those, which require the peer nodes to vote multiple times thereby reaching the consensus even in the presence of byzantine nodes.

Practical Byzantine fault tolerance (PBFT) is an example for above mechanism

Other consensus mechanism follows hybrid approach to combine the process two or more consensus protocols like Pow+PoS which reduces the energy consumption and increases the degree of decentralization.

[5] Given the comparative survey of proof based algorithms like PoW, PoS, DPoS, Proof of Burn(PoB), Proof of Elapsed Time (PoET) taking into the consideration of the mechanism used and parameters of performance metrics such as Scalability, Security, Throughput, Latency, Energy Efficiency.

The author have summarized the consensus mechanism based on proof, which focuses on incentivizing the honest nodes for utilization of their computational power for validating a block.

Analysis done by the author, Byzantine Fault Tolerance based mechanism that guarantees the security in the presence of faulty or malicious nodes, hybrid modes that can collaborate in achieving higher security though maintain efficiency and degree of decentralization. The main criteria involved in analysis and evaluation of these algorithms are performance, scalability and security

[8] Has explained the limitations of consensus algorithms in terms of Scalability, resource wastage, speed of processing the transaction and throughput.

[9] This paper has given the classification of consensus algorithms based on its application in the type of blockchain network like public blockchain, private blockchain, consortium blockchain etc.

Proof of Authority is used in private chain, Consortium blockchain makes use of lightweight Byzantine Fault Tolerance, Public Blockchain uses the consensus of PoW, PoS.

[10] Blockchain technology is decentralized in nature, can tolerate the failure of nodes in its network, ensures data provenance and also enables secure federated data management. The existing consensus mechanism which gives high throughput are generally very expensive, so the authors have proposed a new consensus mechanism that guarantees low latency, high performance and cost effectiveness.

Permissionless blockchain consensus protocol (PoW, PoS) suffer from high computational cost, low throughput and high latency, permissioned blockchain consensus protocol (Byzantine fault tolerance Based) provide high throughput thereby reducing latency.

The authors have proposed a novel consensus mechanism Proof of Execution that promote speed transaction execution and minimalizes the delay in confirmation of these transactions thereby giving the low latency.

PoE is based on speculative execution and single round check commit protocol.

Speculative execution is an optimization technique where the client's transaction requests execution and the result prediction are performed before the transaction is replicated in the local ledger of all the peer nodes. After all the clients accept it then it is committed. If the transaction is found to be guilty or incorrect then it is rolled back to its last committed state of the ledger discarding the speculative results.

PoE will increase the performance as it significantly reduces the waiting time spent for branch resolution and transaction confirmation and efficiently utilizes all the resources by keeping the execution units busy, thus enhancing the computational efficiency.

[1] The authors have proposed a consensus mechanism based Blockchain reputation based consensus (BRBC). This protocols selects the miners having the maximum numbers of reputation votes to add a new block to the chain. A group of judges is randomly selected from the network who rewards the honest miners and penalize the faulty miners.

[5] The main criteria for evaluating these algorithms include performance (throughput), scalability, and security. While PoW is secure, it is energy-inefficient and lacks scalability. PoS is energy-efficient but compromises decentralization. PBFT offers fast transaction confirmations but struggles with scalability due to complexity [25]. The integration of machine learning techniques into consensus protocols is a novel approach to dynamically adjust system parameters and optimize real-time performance. The continuous development and fine-tuning of consensus algorithms are essential to meet evolving requirements and expand the use cases of blockchain technology.

In conclusion, the paper highlights that every consensus algorithm has distinct pros and cons, reflecting the variety of approaches to achieving network consensus. Addressing challenges like transaction speed and energy consumption

remains critical for broader adoption of blockchain technology in real-world applications.

4. Methodology

We have analyzed several research papers majorly focusing on the security and privacy vectors of consensus algorithms. The search was made with the keywords like "blockchain Consensus"+ "security", "consensus" + "Attack", "Consensus" + "protection" was made to several databases of Web of Science, Scopus, Google Scholar, IEEEXplore as well as the journals of Wiley, ACM, Elsevier etc.

This descriptive research have studied and audited the existing consensus protocols and is able to answer the Research Questions like;

RQ1 "Which consensus mechanism is suitable what type of blockchain network?
RQ2 "Whether proof-based consensus algorithms provide better security and scalability over the large blockchain network"?

We have classified the consensus mechanism based on Proof and Acquiescence.
We have classified the consensus mechanism broadly into two categories viz **proof-based** and **acquiescence-based** algorithms, depending on how agreement among distributed nodes is achieved.

1) Proof-Based Consensus Algorithms
Proof-based consensus mechanisms require participating nodes to demonstrate ownership of a **verifiable resource or capability** in order to propose or validate new blocks. The underlying principle is that nodes with greater computational power or contribution to the network have a higher probability of influencing consensus.

2) Acquiescence-Based Consensus Algorithms
Acquiescence-based consensus algorithms rely on **message exchange and agreement protocols** rather than resource proofs. Nodes reach consensus by **voting, quorum formation, or fault-tolerant agreement**, assuming a bounded number of faulty or malicious participants.

Working Principle of Proof based consensus mechanism

A] Proof of Work (PoW): It is frequently used in mining of bitcoin, where the miners in the network are required to solve a complex mathematical puzzle (Hash Function) in order to authorize the block and attach it to the network and also get the rewards in terms of crypto assets. In order to solve the puzzle, the miners need high computational power, resources and it is time consuming. The miners, which has the maximum hash rate and the computational power, will get a chance to mine the block. It also becomes expensive for the attackers as they need to have control over significant network's resources and power in order to alter the block. This is known as 51%attack. Bitcoin and Ethereum uses PoW. [3-4]

B] Proof of Stake (PoS): To overcome the power consumption disadvantage in PoW, PoS was introduced which depends on validators holding a definite volume of stake (Cryptocurrency) to authenticate the transactions for attaching new blocks to the existing chain. One who has larger stake will be given a chance to add the block. Here if in case the selected validator tries to do fraudulent activity or attack the network then that validator will lose the stake. Thus, for each valid transaction the validators are given incentives in the form of stake. In PoS, one of the potential drawback is that the validator which has the maximum will always get a chance to validate the block whereas those with small amount of stake will never get chance to participate in the mining process. PoS has solved this issue by selecting random validators or limiting the amount of cryptocurrency that a single validator can hold. [3-4]

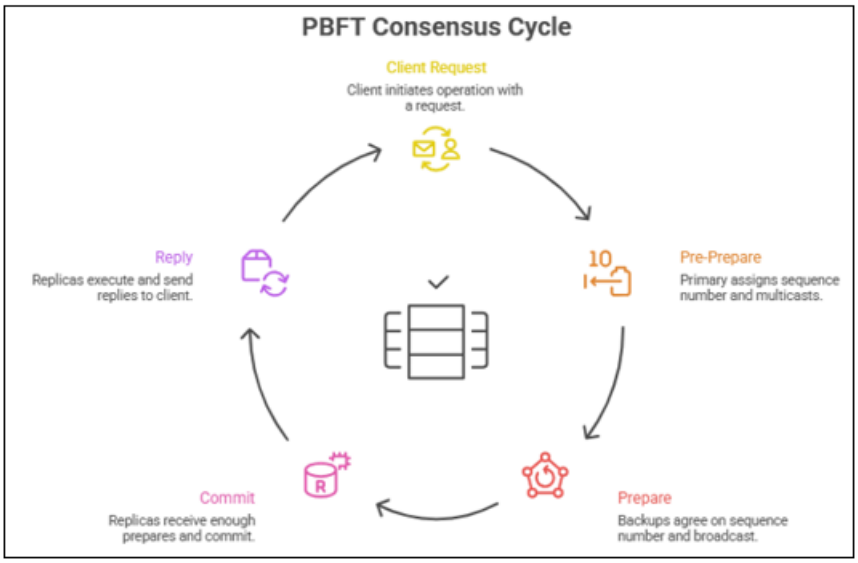
C] Delegated Proof of Work (DPoS): It is an improvement of PoS , where this process relies on a small group of validators known as delegators for validating and adding the new block. All the token holders elect the delegators by implementing the voting method. The more the number of tokens that the delegators have the maximum will be the chance of being selected as validator. This protocol is time and energy efficient as it does not require dependency on the power of individual nodes. The token holders in DPoS are allowed to vote on who to mine new blocks and incentivize the best miners. EOS uses the DPoS Algorithm for consensus mechanism. As it depends on democratic voting model to elect the delegators, it is mandatory to have significant pre-existing peers in the blockchain network. The token holders who have the coins to elect the delegators need to depend upon selected group of delegators making the system centralized. [3-4]

Key characteristics:
- High scalability potential
- Incentive-driven participation
- Probabilistic finality
- Vulnerable to resource centralization

Working Principle of Acquiesce based consensus mechanism

A] **Practical Byzantine Fault Tolerance (PBFT).** It is a protocol designed to work correctly even with the presence of 1/3 rd of the networks with byzantine behaviour. This protocol is quite complex as it requires lot of message overhead to achieve consensus thereby reducing the scalability.

The working of PBFT is as follows:



The client makes the transaction request to the leader node.

Pre-prepare Phase: The leader node after the validation of the request, broadcasts the pre-prepare message of the block/transaction to other peer nodes in the network.
Prepare Phase: The other nodes does the verification of the message broadcasted by the primer or the leader node and sends Prepare message to all other nodes broadcasting it.
Commit Phase: The node commits the message on receiving 2f (twice the number of malicious node + 1) prepare messages.

After receiving 2f+1 commit messages, the node executes the request and sends a reply to the client. Thus, the consensus is achieved when the client receives f + 1 similar replies from the honest nodes. [5]

B] **Proof of Burn (PoB)** : It is a consensus mechanism where the miners burns their coins which are send to irretrievable address known as eater address. The eater address consists of the public key only without the mapping of its private key thereby ensuring that the coin retrieval is impossible. The more the miners burns the coins the more is the probability to become the validator node. The mining power is decided on the number or amount of cryptocurrency burned by the miners.[5]

C] **Proof of Elapsed Time (PoET):** This mechanism relies on the Intel SGX. Every node requires a certificate generate from the trusted authority (Intel) for identity verification and participation in the blockchain network. This mechanism works by assigning a random number to each peer nodes with the help of secured random number generator algorithm. This random number is sleeping or waiting time assigned to the node. The miner nodes then waits until their waiting time is finished and the one who finishes the assigned waiting time first gets a chance to add a new block. The winner node generates the certificate of completion of waiting time and broadcasts this certificate in the blockchain network. The other nodes then verifies the certificates of the winning node and agree upon adding the new block. PoET is used in private and permissioned block where the participants are already known or scrutinized. [5]

Key characteristics:
- Low latency and fast finality
- Strong consistency guarantees
- High communication overhead
- Limited scalability in large networks

Table 1: Comparison of Proof based and Acquiescence based.

Aspect	Proof-Based	Acquiescence-Based
Validation Method	Resource proofs	Message agreement
Fault Tolerance	Economic/security-based	Byzantine or crash-fault tolerant
Finality	Probabilistic	Deterministic
Scalability	High	Moderate to low
Energy Efficiency	Low to high (depends on type)	High
Typical Use	Public blockchains	Permissioned/consortium blockchains

5. Data Analysis and Comparative Study

We have surveyed many research papers for consensus mechanism, which are suitable for types of blockchain, voting-based protocols, BFT-based protocols, reputation-based protocol and have shed the light on the performance of these mechanisms giving the advantages and disadvantages of these mechanisms.

Table 2: Comparative analysis of consensus algorithm on performance metrics

Algorithm	Energy Efficient	Security / Resilience to Attack Vectors	Computational Resources	Stake	Votes	Degree of Decentralization	Scalability	Mechanism
PoW	Low	High (Sybil resistant; vulnerable to 51% attack)	High	NA	NA	High	Low	Solving cryptographic mathematical puzzles
PoS	High	High (Reduced 51% attack risk due to stake requirements)	Medium	Maximum stake	NA	Medium	Medium	Staking a defined amount of cryptocurrency
DPoS	High	Medium–High (Susceptible to centralization and collusion)	Medium	Maximum	High	Low	Medium	Voting for delegates based on stake or reputation
PBFT	High	Very High (Tolerates Byzantine and malicious nodes)	Medium	NA	High	Medium	Low	Message passing and multi-round voting

Mitigating pathways for consensus challenges

The three methods to address the blockchain scalability issues are off-chain solutions, on-chain solutions and consensus algorithms. The on-chain solutions optimizes the transactions or message size. List of on-chain solutions are

1) **Blockchain pipelining**: It divides the validation and transaction-processing task into manageable stages and then executes each stage in parallel.
2) **Blockchain Delivery Network**: It segments the transactions into small chunks, which are then transmitted among nodes within the network. Each node bears the responsibility of validating and processing a segment of transaction, enabling parallel processing and enhancing scalability.
3) Due to this division, it becomes more challenging for malicious actors to compromise the system, as attacking multiple nodes simultaneously becomes more complex.
4) **Block size adjustment**: the idea is to expand the block sizes during network congestion and shrink them during less crowded periods.

The off-chain solutions refer to methods for improving the scalability by taking transactions and data storage of the main blockchain network.

Following are the off-chain solutions

1) **Payment Channel Networks:** In this method, more than two parties open a payment channel amongst themselves to allow to do transactions without broadcasting them to the entire network.
2) **Sharding**: This method involves dividing a blockchain network into smaller entities "Shards" which are responsible for processing a specific portion of the transactions within the network. The main challenges in sharding is to maintain consistency and data integrity across the network.

Lightweight consensus

Lightweight Consensus refers to efficient and resource-conserving consensus mechanisms designed for blockchain systems. These algorithms minimize processing power, communication, and energy overhead, making them suitable for environments with limited resources. Their primary goal is to enable nodes to participate in the consensus process without requiring significant computational or energy resources. In summary, lightweight consensus mechanisms are vital for the evolution of blockchain technology, offering solutions to the inherent limitations of traditional consensus, especially in resource-constrained and large-scale distributed environments. [11]

[12] Highlights that PoS systems offer a significantly more energy-efficient alternative to PoW, supporting a shift towards these mechanisms. While PoS energy consumption varies, it remains moderate and can even undercut traditional payment systems, positioning DLTs as potential contributors to combating climate change

[13] This paper provides a systematic comparison of the formal security aspects of Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus mechanisms in permissionless blockchains. It aims to structure existing knowledge, identify commonalities and discrepancies, and address the trade-offs inherent in these designs The paper highlights inherent trade-offs, such as the dynamic availability-finality dilemma and the availability-accountability dilemma, which cannot be resolved by a single consensus design .while PoW-based consensus with the longest chain rule provides the strongest formal security guarantees, PoS can achieve similar guarantees by addressing its trade-offs through hybrid approaches and specific mitigation strategies. No single solution currently addresses all desired security properties, leading to continuous evolution in blockchain consensus designs

[14] The paper concludes that consensus algorithms are the foundational component of blockchain systems, directly influencing their security and performance. A thorough understanding and comparison of these algorithms are vital for designing robust and efficient blockchain applications in various industrial and societal contexts. The study highlights the trade-offs between consistency, availability, and partition tolerance, emphasizing the need to select appropriate mechanisms based on application requirements.

6. Findings

Every consensus mechanism have some advantages and disadvantages. According to the application area and the type of blockchain, the network needs to decide which consensus mechanism is suitable. Like to make the blockchain network scalable as the chain grows, the network is divided into small shards that process the transaction at their level and then

return the results to the main network after finality reducing the computational overhead, energy requirement etc.

In order to reduce the computations and storage requirements for the peers, checkpoint approach is used to synchronize with the network.

In the Checkpoint approach, the snapshot of the blockchain is taken at certain block height or time interval so that from this point onwards the validation of block can starts instead of again beginning from the genesis block wasting the time and energy. This approach also reduces the resources required to bootstrap a new node and gives recoverability opportunity if there is any interruption in the network.

With the advent of machine learning integration with blockchain techniques, the fine-tuning of the parameter can be done. ML techniques helps in anomaly detection or pattern detection of the node's behavior thereby preventing from malicious attacks increasing the security. [15]

Federated learning is a machine learning techniques, which allows the model to be trained at the local level without sharing the training data to the central authority. FL if integrated with blockchain can mitigate the risk of data breaches and preserve the privacy of the node as the nodes are not required the share any training data in the network.[16]

Table 3: Showcases the challenges of consensus and its mitigation pathways

Consensus Challenges	Mitigation pathways
Scalability	Sharding / offchain solutions, check point approaches
Governance	Incentivizing, on-chain solutions
Energy consumption	Use of PoS, DPoS, PBFT
Privacy and Confidentiality	Zero Knowledge Proofs, Federated Learning

7. Conclusion

Proof-of-Work (PoW) consensus mechanism are broadly used in public blockchains due to its high security but it suffers from the problem of consuming high power in solving the puzzles due to which the it has low latency in confirming the transaction. It also is susceptible to 51% attack.

In order to overcome the problems faced by PoW , Proof of Stake (PoS) was introduced which works on selecting the validators staking more coins in order to become the miner for block validation. Here the machines need not require to utilize more carbon to solve the puzzles so it is definitely more energy efficient but since the chance is always given to the miner with maximum stake the centralization issues arises as rich will become more richer and the miner staking little less coins will never get a chance for adding the block. PoS is also not scalable to larger network.

In order to give fair chances to all the miners Delegated Proof of work (DPoS) came into existence where token holders vote for 'delegates' or 'witnesses' to create new blocks and validate transactions. It is more efficient and scalable than PoW or PoS, but can be more centralized due to power concentrated in a small group of delegates.

Fusion of federated learning and blockchain can empower the consensus mechanism in enhancing the security and privacy of the blockchain. FL can also reduce the computation overheads caused during validation of block and reaching the finality.

We have specified the challenges, which are encountered by various consensus algorithms along with the mitigating techniques as well for future study for the researchers.

Machine learning techniques along with FL can used for optimization of computation resources, fine tuning models, privacy preserving and identification of malicious behavior nodes and to detect them using pattern reorganization.

References

[1] de Oliveira, M. T., Reis, L. H., Medeiros, D. S., Carrano, R. C., Olabarriaga, S. D., & Mattos, D. M. (2020). Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications. *Computer Networks*, *179*, 107367.

[2] Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A., & Colman, A. (2020). Blockchain consensus algorithms: A survey. *arXiv preprint arXiv:2001.07091*.

[3] Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: research and applications, 3(2), 100067.

[4] Jain, A. K., Gupta, N., & Gupta, B. B. (2025). A survey on scalable consensus algorithms for blockchain technology. Cyber Security and Applications, 3, 100065.

[5] Tripathi, P., Singh, D. V., & Pandey, D. H. (2025). A Comprehensive Review of Blockchain Consensus Algorithm. *Available at SSRN 5241590*.

[6] Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A., & Colman, A. (2020). Blockchain consensus algorithms: A survey. *arXiv preprint arXiv:2001.07091*.

[7] ZhigangZhang, JiayiWang*and JinlongWang (2025). A Review of Research on Blockchain Consensus Algorithms, / Procedia Computer Science 262 (2025) 1449–1457

[8] Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017, October). A review on consensus algorithm of blockchain. In *2017 IEEE international conference on systems, man, and cybernetics (SMC)* (pp. 2567-2572). Ieee.

[9] Yang, B. (2024). Review of blockchain's consensus algorithms Comparative Analysis and Future Directions of Blockchain Consensus Mechanisms. *Journal of Computing and Electronic Information Management*, *15*(2), 2024.

[10] Hellings, J., Gupta, S., Rahnama, S., Chen, J., Sana, C., & Sadoghi, M. (2025). Proof-of-Execution: Low-Latency Consensus via Speculative Execution. *ACM Transactions on Database Systems*.

[11] Chacko, N. M., VG, N., Balachandra, M., & T, M. (2025). Lightweight Consensus in Blockchain: A Systematic Literature Review. *ACM Computing Surveys*, *58*(3), 1-37.

[12] Platt, M., Sedlmeir, J., Platt, D., Xu, J., Tasca, P., Vadgama, N., & Ibañez, J. I. (2021, December). The energy footprint of blockchain consensus mechanisms beyond proof-of-work. In *2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 1135-1144). IEEE.

[13] Abellán Álvarez, I., Gramlich, V., & Sedlmeir, J. (2024, April). Unsealing the secrets of blockchain consensus: A systematic comparison of the formal security of proof-of-work and proof-of-stake. In *Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing* (pp. 278-287).

[14] Yadav, A. K., Singh, K., Amin, A. H., Almutairi, L., Alsenani, T. R., & Ahmadian, A. (2023). A comparative study on consensus mechanism with security threats and future scopes: Blockchain. *Computer Communications*, *201*, 102-115.

[15] Chorey, P., & Sahu, N. (2024). Enhancing efficiency and scalability in Blockchain Consensus algorithms: The role of Checkpoint approach. *Journal of Integrated Science and Technology*, *12*(1), 706-706.

[16] Rangwala, M., Venugopal, K. R., & Buyya, R. (2025). Blockchain-Enabled Federated Learning. *arXiv preprint arXiv:2508.06406*.