ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 12, Issue 2, pp: (1-15), Month: October 2025 – March 2026, Available at: www.paperpublications.org

Study and Comparative Analysis of Blockchain Consensus Mechanisms

Dr. N. R. Ananthanarayanan[1], Mr. Suresh Subbu[2]

[1] Professor Department of Computer Science and Applications, SCSMV University

[2] Research Scholar, Dept. of CSA, SCSMV University

DOI: https://doi.org/10.5281/zenodo.17711245

Published Date: 25-November-2025

Abstract: **Blockchain technology is a transformative distributed ledger paradigm that enables secure, transparent, and tamper-resistant data management without centralized authorities. At its core lies the consensus mechanism-the protocol through which distributed nodes agree on a single canonical transaction history. This paper presents a structured review of major blockchain consensus schemes including Proof-of-Work (PoW), Proof-of-Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT), as well as emerging hybrid models such as Avalanche and Polkadot. The analysis evaluates sustainability, scalability, security, and decentralization characteristics, offering a comprehensive comparison across these mechanisms. The findings highlight inherent trade-offs related to energy consumption, throughput, finality, validator governance, and fault tolerance. The study concludes by identifying open research challenges important for designing next-generation blockchain systems capable of supporting large-scale, mission-critical applications.**

Keywords: **Avalanche, Blockchain, Consensus Mechanisms, PBFT, PoS, PoW, Scalability, Security, Sustainability.**

I. INTRODUCTION

Blockchain has witnessed rapid global adoption across domains such as finance, supply chain, manufacturing, healthcare, and digital governance. The global blockchain market is projected to reach USD 469.5 billion by 2030 [1], reflecting the growing demand for decentralized, trustless systems. A blockchain's integrity and performance rely heavily on its consensus mechanism—the algorithm that ensures all nodes agree on valid transactions and maintain a consistent, tamper-evident ledger.

Consensus mechanisms enable trustless networks to maintain consistent and tamper-resistant ledgers without central authorities. For example, Bitcoin, introduced by Nakamoto in 2008 [2], pioneered decentralized consensus through Proof-of-Work (PoW), demonstrating that adversarial participants can be economically disincentivized from attacking the system. However, PoW's limitations in scalability and sustainability have accelerated the development of alternative mechanisms such as Proof-of-Stake (PoS), PBFT, and hybrid models like Avalanche and Polkadot.

This paper systematically reviews and analyzes PoW, PoS, PBFT, Avalanche, and Polkadot, highlighting trade-offs and open research directions. It presents their architectural principles, performance characteristics, and suitability for different blockchain environments, along with a comparative analysis across dimensions such as energy consumption, scalability, security, and decentralization.

II. PROOF-OF-WORK (POW)

A. Technical Overview

In PoW, network participants (miners) expend computational effort to propose the next block. Miners repeatedly compute SHA-256 hashes over block headers while varying a nonce until they find a hash below a protocol-defined target. This

process can be viewed as solving a cryptographic "puzzle" that is hard to compute but easy for others to verify. The network periodically adjusts the difficulty of this puzzle (every 2016 blocks in Bitcoin, roughly every two weeks) so that blocks continue to be found at an average target time of roughly 10 minutes.

Each block contains the hash of the previous block, forming a linked chain. Because each block's hash depends on the previous block's contents, altering any block would require recomputing the PoW for that block and all subsequent blocks. Under honest-majority assumptions, this makes history revisions computationally infeasible unless an attacker controls more than half of the total network hash rate—the so-called 51% attack threshold.

B. Example – Bitcoin

Bitcoin is the canonical Proof-of-Work blockchain, relying on SHA-256 hashing and an average block interval of approximately 10 minutes. Each new block provides a block reward and transaction fees to the successful miner, creating a strong economic incentive to maintain network security and participate honestly. The Cambridge Bitcoin Electricity Consumption Index estimates Bitcoin's annual electricity demand at roughly 70.4 TWh in 2023, equivalent to about 0.38% of global electricity usage, underscoring the significant energy intensity of PoW [3]. Earlier studies recorded even higher values, such as ~121 TWh in 2020, further illustrating the substantial environmental footprint associated with continuous mining operations.

Bitcoin's throughput remains limited due to its fixed block size of ~1 MB and 10-minute block interval, supporting only 3–7 transactions per second (TPS). Finality in Bitcoin is probabilistic: the deeper a transaction is embedded within the chain, the more secure it becomes. A transaction is conventionally considered final after six confirmations, which typically corresponds to about one hour. Temporary forks may occur when two miners produce valid blocks simultaneously, but the longest-chain rule ensures eventual consistency as subsequent blocks reinforce one branch over the other.

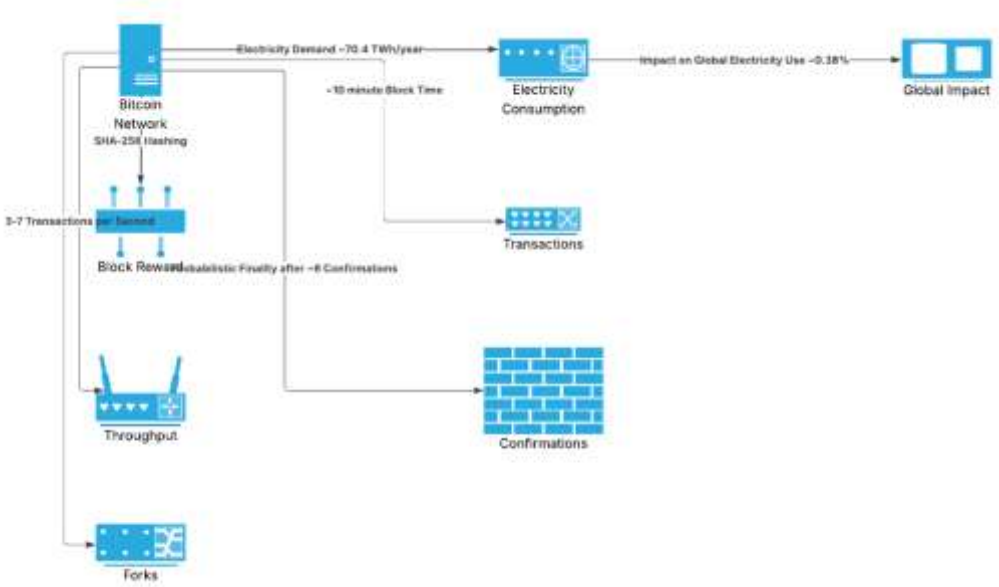

Fig. 1 N/W Illustration of PoW Example

C. PoW Advantages

- **Security:** PoW is battle-tested; altering the ledger requires enormous computational power. Without a majority of hash rate, double-spends become virtually impossible, deterring censorship and tampering.
- **Simplicity and Openness:** Anyone with suitable hardware can attempt to mine (permissionless participation). Over time, PoW has developed a mature infrastructure of miners, ASIC manufacturers, and mining pools with a clear incentive model.
- **Proven Economic Model:** The combination of block rewards, transaction fees, and difficulty adjustment is well understood, providing predictable issuance and security dynamics.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 12, Issue 2, pp: (1-15), Month: October 2025 – March 2026, Available at: www.paperpublications.org

D. PoW Drawbacks

- **Energy Intensive:** By design, PoW converts vast amounts of electrical energy into cryptographic security. Bitcoin alone consumes tens of TWh per year [3]. This raises environmental and sustainability concerns at global scale.
- **Limited Throughput:** PoW chains such as Bitcoin and early Ethereum have low transaction capacity (3–15 TPS) and relatively long confirmation times (minutes), constraining high-volume applications.
- **Centralization Pressures:** Specialized ASIC hardware and large-scale mining farms dominate hashing power. A handful of large mining pools control most Bitcoin block production, introducing centralization risk.
- **Probabilistic Finality:** PoW provides only eventual finality. Network reorganizations can occur, and deep reorgs, while rare, remain a theoretical risk under large-scale attacks.

Fig. 2 PoW Mind Map

E. Proof-of-Work (PoW) Architecture

Key Components:

- **Miners:** Compete to solve cryptographic puzzles (e.g., SHA-256) to propose blocks.
- **Full Nodes:** Validate transactions and blocks and maintain full copies of the blockchain.
- **Transaction Pool (Mempool):** Stores unconfirmed transactions awaiting inclusion in a block.
- **Blockchain:** A linked list of blocks secured via cryptographic hashes.
- **Consensus Rules:** Include the longest-chain rule, difficulty adjustment, block size/weight limits, and reward schedules.

Workflow:

1. **Transaction Propagation:** Users broadcast transactions to the network.
2. **Block Creation:** Miners select transactions from the mempool, assemble a candidate block, and attempt to solve the PoW puzzle.
3. **Validation:** Once a miner finds a valid hash, the block is broadcast; nodes verify PoW and all transactions.
4. **Chain Extension:** Valid blocks are appended to the longest chain; miners begin working on top of the new tip.

Security Mechanisms:

- **Economic Incentives:** Block rewards and transaction fees incentivize honest behavior.
- **Difficulty Adjustment:** Maintains a steady block interval despite changing total hash power.
- **51% Attack Resistance:** Security depends on honest miners controlling the majority of hash power.

Scalability Challenges:

- **Low Throughput:** Fixed block size and interval limit TPS.
- **Latency to Finality:** Multiple block confirmations are required to reach high confidence.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 12, Issue 2, pp: (1-15), Month: October 2025 – March 2026, Available at: www.paperpublications.org

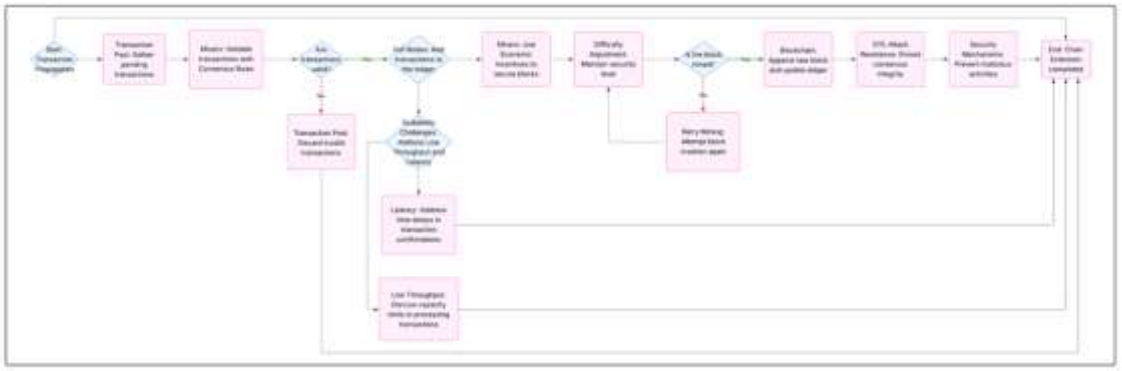

Fig. 3 PoW Workflow

III. PROOF-OF-STAKE (POS)

A. Technical Overview

PoS replaces energy expenditure with economic stake. Instead of miners, the network has validators who must deposit (stake) some amount of cryptocurrency to participate in block proposal and validation. The protocol pseudorandomly selects validators (with probability proportional to stake) to propose and attest to blocks. Misbehavior—such as double-signing or creating conflicting blocks—can result in slashing, where a portion of the validator's stake is destroyed.

In modern PoS designs, time is divided into discrete slots and epochs. In each slot, a validator is chosen to propose a block, while a committee of other validators attests to its validity. Once a supermajority (e.g., ≥2/3 of staked weight) votes in favor, blocks or checkpoints can be finalized. Many PoS systems therefore provide deterministic or near-deterministic finality.

B. Example – Ethereum (Post-Merge)

Ethereum completed its PoW-to-PoS "Merge" in September 2022, moving to a Beacon Chain–based PoS consensus. Validators are required to stake 32 ETH to run a validating node. As of mid-2024, approximately 32.5 million ETH (~27% of the total supply) is staked, representing well over one million validator slots. The switch to PoS reduced Ethereum's energy usage by ~99.95% [4], making it roughly 2000× more energy efficient than its prior PoW regime.

Pre-Merge, Ethereum supported ~10–15 TPS with high gas fees during congestion. While the Merge itself did not immediately increase base-layer TPS, it enabled an architectural roadmap that includes sharding and widespread use of layer-2 rollups. These mechanisms are expected to raise effective throughput to tens or hundreds of thousands of TPS over time. Ethereum's finality is now deterministic at the checkpoint level: once a supermajority of validators attest to a given checkpoint, it is final and cannot be reverted without slashing a substantial amount of stake.

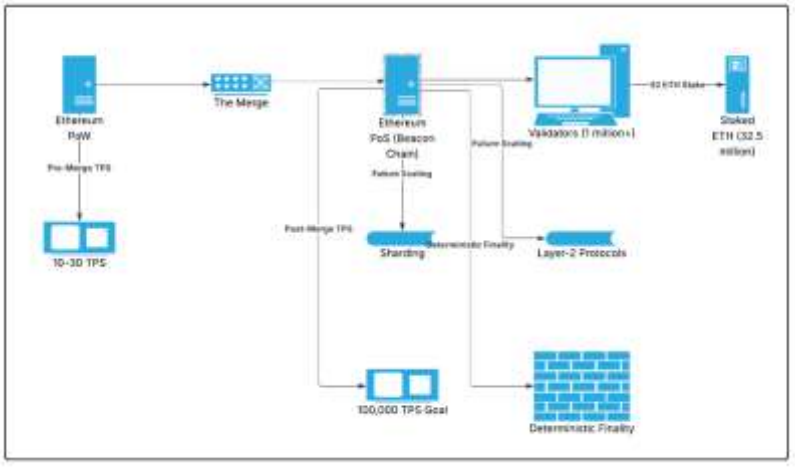

Fig. 4 N/W Illustration of PoS Example

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 12, Issue 2, pp: (1-15), Month: October 2025 – March 2026, Available at: www.paperpublications.org

C. PoS Advantages

- **Energy Efficiency:** PoS virtually eliminates wasteful computation. Ethereum's energy use dropped by ~99.95% after the Merge [4].
- **Scalability Potential:** Faster block times (e.g., 12-second slots) and compatibility with sharding and rollups support higher throughput.
- **Economic Security:** Attacks require control of a majority of staked tokens, which is expensive and self-destructive because it devalues the attacker's holdings.
- **Broader Participation:** Staking pools and liquid staking protocols allow participants with smaller balances to share rewards.

D. PoS Drawbacks

- **Wealth Centralization:** Large exchanges and staking providers can accumulate disproportionate stake. For example, a small number of entities control a majority of staked ETH.
- **Complexity and Maturity:** PoS requires sophisticated mechanisms for randomness, slashing, validator rotation, and fork choice, increasing implementation risk.
- **Nothing-at-Stake (Mitigated):** Early theoretical concerns suggested validators might sign on multiple forks at negligible cost. Modern PoS designs mitigate this using slashing and strict fork-choice rules, but the design space remains complex.
- **Indirect Contribution to Security:** Security is based on economic stake rather than visible physical cost, which some argue makes attacks more abstract and dependent on market dynamics.

Fig. 5 PoS Mind Map

E. Proof-of-Stake (PoS) Architecture

Key Components:

- **Validators:** Nodes that stake tokens to participate in block proposal and validation.
- **Staking Contracts:** On-chain contracts that lock stake and define reward/slashing conditions.
- **Beacon Chain (e.g., Ethereum):** Coordinates validators, assigns committees, and may manage shard chains.
- **Shards or Parallel Chains:** Optional parallel chains that increase throughput by distributing state and computation.

Workflow:

1. **Validator Selection:** Validators are pseudorandomly chosen based on stake distribution.
2. **Block Proposal:** The selected validator proposes a block for a given slot or shard.
3. **Attestations:** A committee of validators votes on the block's validity via cryptographic signatures.
4. **Finalization:** Once enough attestations are collected (e.g., ≥2/3), checkpoints or blocks are finalized through a finality gadget such as Casper FFG.

Security Mechanisms:

- **Slashing:** Validators lose stake for equivocation, downtime, or other malicious behavior.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 12, Issue 2, pp: (1-15), Month: October 2025 – March 2026, Available at: www.paperpublications.org

- **Finality Gadgets:** Protocols such as Casper FFG provide strong finality guarantees once a supermajority locks in a checkpoint.
- **Anti-Centralization Features:** Some designs include stake caps, dynamic rewards, or governance constraints to limit dominance by large holders.

Scalability Features:

- **Sharding:** Splits the network into multiple shards to process transactions in parallel.
- **Faster Block Times:** Sub-minute or sub-second block times are possible due to lack of heavy PoW puzzles.

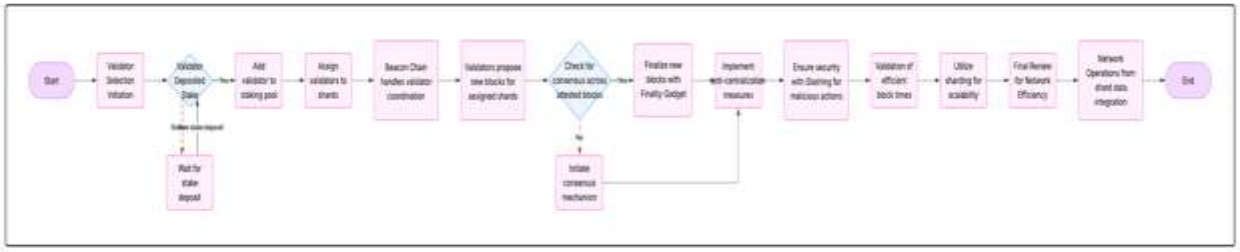

Fig. 6 PoS Workflow

IV. PBFT

A. Technical Overview

PBFT is a consensus algorithm designed for permissioned networks with known validator identities. Originally proposed by Castro and Liskov (1999) [6], PBFT addresses the Byzantine Generals Problem in practical distributed systems. The protocol assumes a fixed set of validators (replicas), where one acts as the leader (primary) and the others as backups.

Consensus proceeds in three main phases: Pre-Prepare, Prepare, and Commit. The leader proposes a block in the Pre-Prepare phase, validators broadcast Prepare messages after verifying the proposal, and then broadcast Commit messages once they receive sufficient Prepare votes. When at least 2f+1 of the 3f+1 validators (more than two-thirds) commit, the block is finalized. PBFT tolerates up to f Byzantine (malicious or faulty) validators out of 3f+1.

B. Example – Hyperledger Fabric (SmartBFT)

Hyperledger Fabric, an enterprise blockchain framework under the Linux Foundation, employs PBFT-style ordering services. In Fabric v3.0, SmartBFT was introduced as a BFT ordering service for transaction sequencing. Ordering service nodes (often one per organization) run this consensus to generate blocks. Fabric guarantees deterministic finality: once a block is created and disseminated by the orderer, it is final and cannot be reverted.

Performance evaluations show that SmartBFT can process thousands of TPS in small clusters—for instance, around 2000 TPS in a 4-node configuration—with latencies on the order of a few seconds. Fabric's explicit finality and permissioned structure make it suitable for use cases such as supply chain, finance, and inter-organizational data coordination.

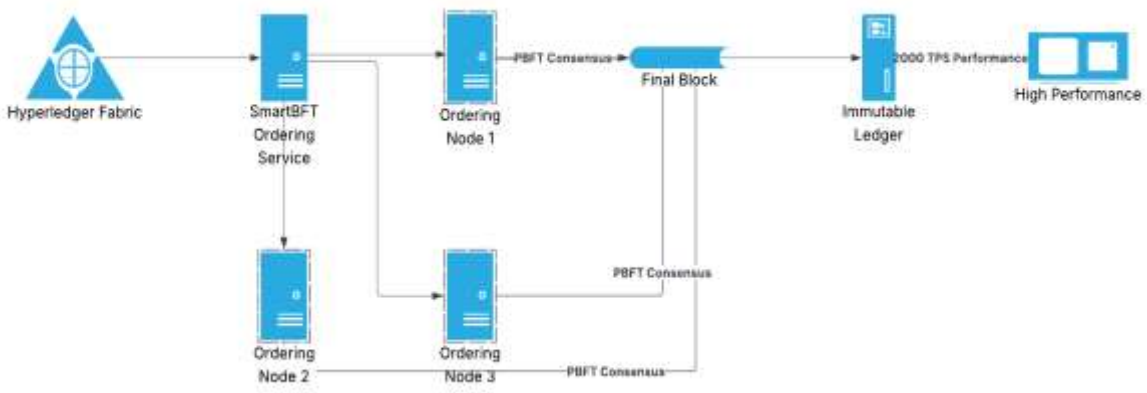

Fig. 7 N/W Illustration of SmartBFT Example

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 12, Issue 2, pp: (1-15), Month: October 2025 – March 2026, Available at: www.paperpublications.org

C. PBFT Advantages

- **Deterministic Finality:** Every consensus round produces a single canonical block; once committed, the block cannot be reverted.
- **High Throughput (Small Networks):** PBFT achieves high TPS for small to medium validator sets.
- **Low Energy Usage:** No energy-intensive puzzles or mining; nodes perform only standard computation and message exchanges.
- **Strong Consistency:** As long as fewer than one-third of validators are Byzantine, PBFT guarantees safety and liveness.

D. PBFT Drawbacks

- **Scalability Limits:** PBFT's $O(n^2)$ communication overhead makes it difficult to scale to hundreds or thousands of validators.
- **Permissioned Requirement:** PBFT assumes known, authenticated validators, making it less suitable for fully open public networks.
- **Operational Complexity:** Managing membership, performing leader rotations, and handling dynamic validator sets add complexity.
- **Partial Byzantine Tolerance:** If $\geq 1/3$ of validators collude or fail maliciously, consensus safety and liveness can be compromised.

Fig. 8 PFBT Mind Map

E. PBFT Architecture

Key Components:

- **Validator Set:** A fixed, permissioned set of nodes (e.g., organizations in a consortium).
- **Membership Service:** Authenticates validators and manages cryptographic identities.
- **Client Nodes:** Submit transactions to the network and receive responses.

Workflow:

1. **Request:** A client sends a transaction to the primary.
2. **Pre-Prepare:** The primary proposes a block and broadcasts it to all validators.
3. **Prepare:** Validators verify the proposal and broadcast Prepare messages.
4. **Commit:** After receiving $\geq 2/3$ matching Prepare messages, validators broadcast Commit messages.
5. **Reply:** Once a validator collects enough Commit messages, it finalizes the block and replies to the client.

Security Mechanisms:

- **Byzantine Fault Tolerance:** Tolerates up to one-third malicious nodes.
- **View Change:** If the primary is suspected of misbehavior or failure, a view-change protocol elects a new leader.
- **Deterministic Finality:** Ensures no forks; once a block is committed, all honest nodes agree on the ledger state.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 12, Issue 2, pp: (1-15), Month: October 2025 – March 2026, Available at: www.paperpublications.org

Scalability Constraints:

- **O(n^2) Messages:** Communication cost rises quadratically with validator count.
- **Centralized Governance:** Validator admission and removal are centrally managed, which can introduce governance challenges.

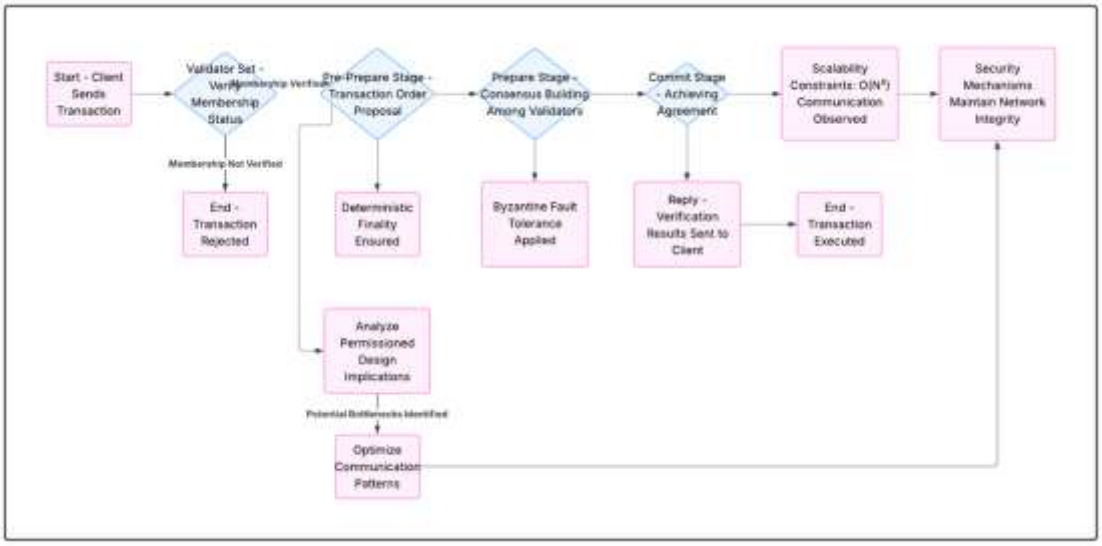

Fig. 9 PBFT Workflow

V. EMERGING HYBRID MODELS

A. Avalanche

Avalanche introduces a metastable, sampling-based consensus protocol. Instead of all-to-all communication, nodes repeatedly query small, random subsets of validators to determine network preference for a transaction or block. Over repeated rounds, the network converges to a global preference with high probability.

Avalanche supports over 3000 TPS with sub-second finality in benchmarks [7]. It leverages a DAG (X-Chain) for asset transfers and a linear Snowman chain for smart contract execution (e.g., C-Chain), all secured by a PoS-based staking model.

Strengths:

- Highly scalable due to subsampling (O(k log N) complexity).
- Energy efficient, relying on PoS rather than PoW.
- Sub-second probabilistic finality.

Challenges:

- Security remains probabilistic and requires long-term empirical validation.
- Subnet validators may centralize around well-capitalized actors.

Fig. 10 Avalanche Mind Map

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 12, Issue 2, pp: (1-15), Month: October 2025 – March 2026, Available at: www.paperpublications.org

Avalanche Consensus Architecture – Key Components:

- **Validators:** Stake tokens to participate in sampling-based consensus.
- **Transaction DAG (X-Chain):** Non-linear structure enabling high parallelism for asset transactions.
- **Snowman Protocol (C-Chain):** Linearized consensus optimized for smart contracts.
- **Subsampling Engine:** Randomly selects validators to query in each round.
- **Virtual Machine (VM):** Executes application logic on subnets.

Workflow:

1. **Transaction Submission:** Clients broadcast transactions to validators.
2. **Random Sampling:** Validators query a small, random subset of peers (e.g., $k \approx 20$).
3. **Voting:** Peers respond with their preferred transaction or branch.
4. **Metastability:** Repeated sampling rounds reinforce a dominant preference.
5. **Finality:** When the confidence threshold is met, decisions become effectively irreversible.

B. Polkadot

Polkadot employs a heterogeneous multi-chain architecture secured by a central Relay Chain and Nominated Proof-of-Stake (NPoS). Independent parachains plug into the Relay Chain and benefit from shared security. GRANDPA (GHOST-based Recursive Ancestor Deriving Prefix Agreement) provides BFT-style finality [8].

Strengths:

- Parallel execution across up to 100+ parachains, significantly increasing network throughput.
- Strong cross-chain interoperability via XCMP (Cross-Chain Message Passing).
- Deterministic finality through GRANDPA, with 12–60 second finalization times.

Challenges:

- Limited validator set size (e.g., a few hundred validators for many parachains).
- Governance and upgrade complexity.
- Potential Relay Chain bottlenecks.

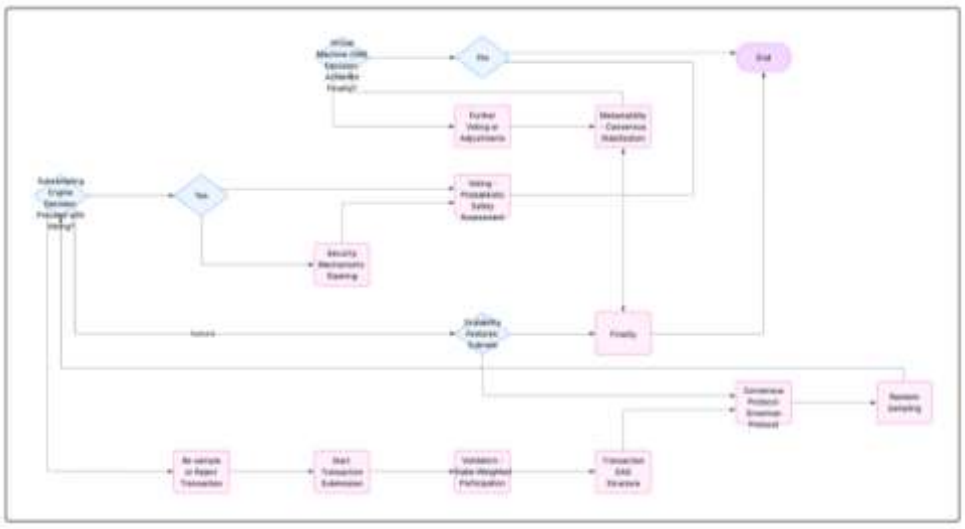

Fig. 11 Avalanche Workflow

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 12, Issue 2, pp: (1-15), Month: October 2025 – March 2026, Available at: www.paperpublications.org

Polkadot Consensus Architecture – Key Components:

- **Relay Chain:** Central chain responsible for security and finality.
- **Parachains:** Independent blockchains that process transactions in parallel.
- **Collators:** Nodes that maintain parachains and propose candidate blocks to validators.
- **Validators:** Secure the Relay Chain using NPoS and validate parachain blocks.
- **Nominators:** Stake DOT to support trustworthy validators.
- **Fishermen:** Monitor and report malicious behavior.
- **XCMP:** Protocol enabling secure cross-chain messaging between parachains.

Fig. 12 Polkadot Mind Map

Workflow:

1. **Parachain Block Creation:** Collators collect transactions and propose parachain blocks.
2. **Relay Chain Validation:** Validators verify parachain block validity and include them in the Relay Chain.
3. **GRANDPA Finality:** Validators vote to finalize blocks in batches.
4. **Cross-Chain Messaging:** Parachains communicate via XCMP, allowing interoperability.

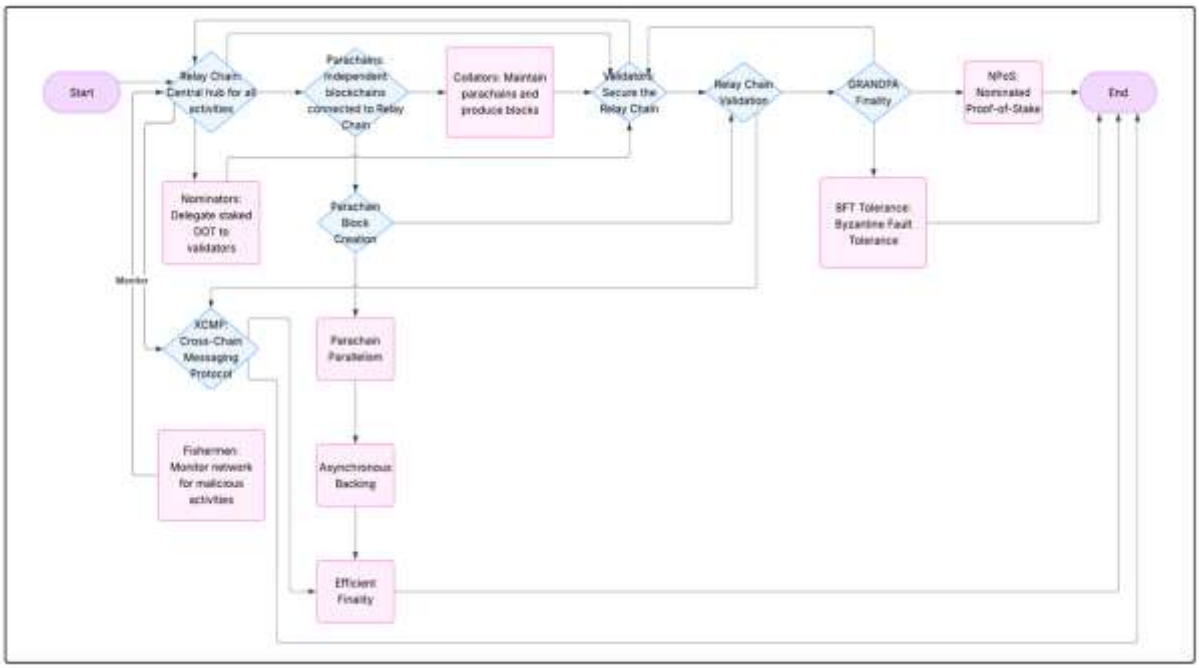

Fig. 13 Polkadot Workflow

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 12, Issue 2, pp: (1-15), Month: October 2025 – March 2026, Available at: www.paperpublications.org

VI. COMPARATIVE ANALYSIS OF CONSENSUS MECHANISMS

Aspect	PoW	PoS	PBFT
Consensus	Hash puzzles (SHA-256)	Stake-based selection	Multi-round voting
Finality	Probabilistic (6+ blocks)	Checkpoint-based finality	Immediate, determinis
Throughput	Low (~7 TPS)	High (1000+ TPS with sharding)	High (1000+ TPS)
Energy Use	High (70+ TWh annually)	Low (99% reduction vs. PoW)	Minimal
Validator Set	Permissionless (open mining)	Permissionless (open staking)	Permissioned (fixed nc
Use Case	Public, decentralized ledgers	Eco-friendly public chains	Consortium/enterprise

Aspect	Avalanche	Polkadot
Consensus	Repeated subsampled voting	Hybrid NPoS + GRANDPA BFT
Finality	Probabilistic (sub-second)	Deterministic (12–60 seconds)
Throughput	High (3000+ TPS)	High (1000–10,000 TPS with parachains)
Energy Use	Low (PoS-based)	Low (PoS-based)
Validator Set	Permissionless (open staking)	Permissioned (limited slots)
Scalability Core	DAG + Subsampling	Parachains + Relay Chain
Use Case	High-speed public chains	Interoperable multi-chain ecosystems

Fig. 14 Comparative Analysis

A structured comparison of PoW, PoS, PBFT, Avalanche, and Polkadot reveals:

- **PoW:** Extremely secure but energy-intensive with low throughput and probabilistic finality.
- **PoS:** Greatly improves sustainability and enables higher throughput but raises concerns about stake centralization and protocol complexity.
- **PBFT:** Offers deterministic finality and high throughput for small, permissioned networks but does not scale well to large public settings.
- **Avalanche:** Achieves very high throughput and fast probabilistic finality via sampling but requires deeper analysis of long-term security under adversarial conditions.
- **Polkadot:** Provides horizontal scalability and interoperability through parachains and shared security, but introduces governance and architecture complexity.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 12, Issue 2, pp: (1-15), Month: October 2025 – March 2026, Available at: www.paperpublications.org

VII. 5-DIMENSIONAL COMPARATIVE ANALYSIS

TABLE 1. 5-Dimensional Comparison

Metric	PoW	PoS	PBFT
Energy Consumption	**High.** Networks consume massive electricity (e.g. Bitcoin ~70 TWh/yr, which is ~0.38% of world use). Mining pools and ASICs dominate power use.	**Very low.** Only validators' computers run (no wasteful mining). Ethereum reports a ~99.95% drop in energy after moving to PoS (~2000× more efficient than PoW).	**Low.** No mining; nodes only do standard computation and messaging. Comparable to other BFT systems; energy use scales with server count.
Throughput / Scalability	**Low.** Bitcoin ~3–7 TPS, Ethereum PoW ~10–15 TPS. Block times are minutes long. Scaling often requires off-chain solutions.	**Moderate to High.** Ethereum now ~15–30 TPS (similar to PoW era), but future sharded PoS aims for thousands to ~100,000 TPS. Latency is moderate (seconds) but improves with upgrades.	**High (small n).** Fabric's BFT can achieve thousands of TPS (e.g. ~2000 TPS @4 nodes). Throughput remains high for tens of nodes; adds overhead for large n. Latency to finality is low (one or two rounds of messaging).
Finality / Latency	**Probabilistic.** New blocks depth increases confidence. For Bitcoin, 6 blocks (~1 hour) is conventionally "final". Latency ~10 minutes per block.	**Deterministic (in many designs).** Ethereum's Casper finalizes epochs (~6.4 minutes per epoch), with strong finality once a supermajority agrees. No lingering forks once final. Average block time ~12s.	**Immediate.** Consensus in each round yields a single canonical block with no forks. Once a block is committed, it is final (as in Hyperledger Fabric). Latency is on the order of seconds (network and processing delays).
Fault Tolerance	**Up to 51%.** An attacker must control >50% of total hashpower to rewrite history (very costly). Otherwise, the chain with most proof-of-work wins.	**Up to 51%.** Attacker needs >50% of staked coins to subvert the chain (an extremely high economic barrier). Moreover, attacking validators lose stake via slashing.	**Up to 33%.** PBFT tolerates up to f faults out of n=3f+1 nodes . If ≥33% are Byzantine, safety/liveness can fail. (Requires known identities.)
Decentralization	**Permissionless (public).** Anyone with hardware can join. However, mining tends to centralize among large pools/ASIC owners. Geographic or pool centralization can occur.	**Permissionless (public).** Anyone with minimum stake (e.g. 32 ETH) can become a validator. Staking pools aggregate small holders. Centralization concerns arise if few large entities control most stake (e.g. top 4 stakeholders ~54% of staked ETH).	**Permissioned (private consortium).** Only known validators (e.g. organizations) can join. This naturally limits decentralization but enables trust (or accountability) in validator behavior.

MECHANISM	SUSTAINABILITY	SCALABILITY	SECURITY	DECENTRALIZATION
POW	Very low	Low	High (if hash power honest)	Moderate (mining pools)
POS	High	High	Medium to High (slashing critical)	Moderate (wealth concentration)
PBFT	High	High (small networks)	High (if ≤ 1/3 malicious)	Low (permissioned)
AVALANCHE	High	Very High	High (probabilistic)	High
POLKADOT	High	Very High (sharding)	High	Moderate

1) Sustainability (Energy Consumption)

- **PoW:** High energy consumption (e.g., Bitcoin ~70 TWh/year, ~0.38% of global usage).
- **PoS:** Very low energy use; Ethereum reports a ~99.95% drop post-Merge [4].
- **PBFT:** Low energy usage; only standard computation and messaging.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 12, Issue 2, pp: (1-15), Month: October 2025 – March 2026, Available at: www.paperpublications.org

- **Avalanche & Polkadot:** PoS-based and highly energy efficient.

2) Throughput / Scalability

- **PoW:** Low; Bitcoin ~3–7 TPS, Ethereum PoW ~10–15 TPS.
- **PoS:** Moderate to high; post-Merge Ethereum ~15–30 TPS today, with sharding/rollups targeting much higher.
- **PBFT:** High for small n; thousands of TPS in 4–20 node networks.
- **Avalanche & Polkadot:** Very high; Avalanche reports 3000+ TPS, while Polkadot scales via parachain parallelism.

3) Finality / Latency

- **PoW:** Probabilistic; ~6 blocks (~1 hour) for strong confidence.
- **PoS:** Deterministic or near-deterministic; Ethereum's Casper finality gadget finalizes epochs within minutes.
- **PBFT:** Immediate deterministic finality after each consensus round.
- **Avalanche:** Sub-second probabilistic finality.
- **Polkadot:** Deterministic finality via GRANDPA within tens of seconds.

4) Fault Tolerance

- **PoW:** Secure as long as <50% of hash power is controlled by an attacker.
- **PoS:** Secure as long as attackers control <50% of stake (and are subject to slashing).
- **PBFT:** Tolerates up to 1/3 Byzantine nodes.
- **Avalanche & Polkadot:** Similar BFT-style assumptions, often with ≤1/3 Byzantine thresholds.

5) Decentralization

- **PoW:** Permissionless but prone to mining pool centralization.
- **PoS:** Public and permissionless, yet susceptible to wealth concentration.
- **PBFT:** Permissioned, with low decentralization by design.
- **Avalanche:** Aims for high validator participation via PoS.
- **Polkadot:** Moderately decentralized but constrained by validator set size.

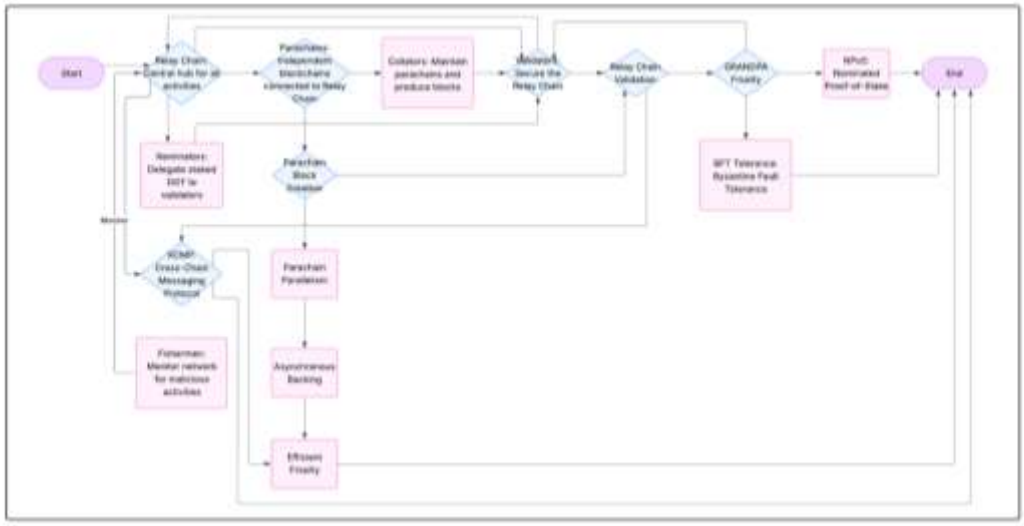

Fig. 15 BFT Workflow

VIII. EXAMPLES / USE CASES

- **PoW:**
  - Open public cryptocurrencies: Bitcoin, Litecoin, Monero, early Ethereum.
  - Best suited for maximal censorship resistance and conservative monetary systems.
- **PoS:**
  - Modern public and hybrid networks: Ethereum 2.0, Cardano, Polkadot, Tezos, Cosmos (Tendermint), Solana.
  - Target applications requiring high throughput and lower environmental impact.
- **PBFT:**
  - Enterprise and consortium blockchains: Hyperledger Fabric (IBM, Walmart), R3 Corda (with BFT variants), permissioned Tendermint/Cosmos deployments.
  - Ideal where participants are known and strong finality is required (e.g., interbank settlements, supply chain auditing).
- **Hybrid Models (Avalanche, Polkadot):**
  - High-throughput DeFi platforms, interoperable cross-chain applications, and large-scale multi-chain ecosystems.

IX. CONCLUSION

Blockchain consensus mechanisms continue to evolve in response to the growing need to balance sustainability, security, scalability, and decentralization—four dimensions that define the long-term viability of distributed ledger technologies. Proof-of-Work (PoW) remains the historical benchmark for decentralized security due to its well-studied resilience against adversarial attacks and its straightforward economic model. However, the inherent energy consumption and hardware dependence associated with PoW limit its feasibility as a scalable, environmentally responsible solution for future global applications. As blockchain adoption increases, this limitation becomes a significant barrier to widespread institutional deployment.

Proof-of-Stake (PoS) addresses many of PoW's sustainability concerns by replacing computational work with economic staking. This shift drastically reduces energy consumption and enables faster block times, improved throughput, and compatibility with sharding and rollup-based scaling techniques. Nevertheless, PoS introduces new challenges—such as stake centralization, governance influence by large token holders, and the need for robust slashing and randomness mechanisms. These factors highlight the importance of designing fair and transparent validator incentives to maintain decentralization.

Practical Byzantine Fault Tolerance (PBFT), with its deterministic finality and high throughput, remains well-suited for permissioned or enterprise applications where validator identities are known and performance requirements are stringent. However, PBFT's communication overhead limits its use in large-scale public networks.

Emerging hybrid models such as Avalanche and Polkadot demonstrate how modular, interoperable architectures can push blockchain scalability beyond the constraints of traditional designs. Avalanche's metastable consensus and Polkadot's heterogeneous multi-chain framework both indicate promising directions for next-generation systems.

Future research must emphasize formal security proofs, fault-tolerant governance models, effective validator management, cross-chain interoperability, and rigorous real-world stress testing. Addressing these challenges will ensure that future blockchain platforms remain secure, sustainable, and adaptable enough to support complex, mission-critical applications across diverse industries.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to SCSMV University for providing the academic support and research environment necessary for this work. We extend heartfelt thanks to the Department of Computer Science and Applications (CSA) for their continuous encouragement and access to essential resources. The authors also acknowledge the invaluable guidance and mentorship of **Dr. N. R. Ananthanarayanan**, whose supervision, technical insights, and

constructive feedback significantly contributed to the quality and clarity of this research. Special thanks are extended to colleagues, research peers, and all individuals who provided critical comments and suggestions during the preparation of this manuscript. Their contributions have greatly strengthened the overall work.

REFERENCES

[1] "Blockchain Market Size, Share & Trends Analysis Report," GlobeNewswire, 2023.

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[3] A. de Vries, "Bitcoin's Growing Energy Problem," *Joule*, vol. 2, no. 5, 2018, pp. 801–805.

[4] "Ethereum Energy Consumption After Merge," Ethereum Foundation, 2022.

[5] J. Garay, A. Kiayias, and N. Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications," in *Advances in Cryptology – EUROCRYPT 2015*, pp. 281–310.

[6] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI)*, 1999.

[7] E. Gün Sirer, V. Sekniqi, et al., "Avalanche: A Novel Metastable Consensus Protocol Family for Blockchains," arXiv:1906.08936, 2019.

[8] G. Wood, "Polkadot: Vision for a Heterogeneous Multi-Chain Framework," 2016.