Supereum: A Hybrid PoW-PoS Blockchain with an Integrated Smart Wallet for Secure and Efficient Transactions

# Dr. V. Geeta

*dept. of Cyber Security SNIST*

Hyderabad, India [geeta.v@sreenidhi.edu.in](mailto:geeta.v@sreenidhi.edu.in)

# Pranay Kalekar

*dept. of Cyber Security SNIST*

Hyderabad, India [prokalekar2003@gmail.com](mailto:prokalekar2003@gmail.com)

# Surabhi Suprith Vardhan Rao

*dept. of Cyber Security SNIST*

Hyderabad, India [suprithsurabhi@gmail.com](mailto:suprithsurabhi@gmail.com)

Barruri Sai Suhas Sharma *dept. of Cyber Security SNIST*

Hyderabad, India [saisuhas1212@gmail.com](mailto:saisuhas1212@gmail.com)

***Abstract*—In the rapidly developing world of digital trans- actions, blockchain technology has become a game changer, providing decentralization, security, and transparency. However, many blockchain systems are currently facing challenges such as high transaction costs and unfriendly features, which make them less realistic for daily use. To solve these problems, we propose a hybrid blockchain system combining proof of work (POW) and proof of stake (POS), ensuring both safety and energy efficiency. At the same time, we introduce a functional digital investment portfolio designed to simplify transactions among colleagues. The star function of the portfolio is the ability to facilitate requests based on requirements, similar to the features found in UPI systems. Users can send, receive, and request payments transparently and access their trading history to better monitor their finances. The hybrid blockchain is optimized for low transactions through an aerodynamic cost system, eliminating the need for complex smart contracts. By developing our own blockchain, we ensure transparency and integration with the portfolio, allowing buttons to directly interact and providing more flexibility in the system design. This project aims to fill the gap between advanced blockchain technology and its similarities, providing a safe, profitable and friendly solution for digital transactions. The combination of a hybrid blockchain and a visual portfolio with unique characteristics makes this system a practical choice for daily use of cryptocurrencies, paving the way for wider applications than the public. Blockchain technology.**

***Index Terms*—Hybrid Blockchain, Proof of Work, Proof of Stake, Digital Wallet, Cryptocurrency Transactions, Decen- tralized Finance, Transaction Cost Optimization, Blockchain Transparency, UPI-based Payments, Energy-efficient Blockchain, Blockchain Usability, Secure Digital Transactions**

1. Introduction

Blockchain technology has completely transformed digital transactions by ensuring decentralization, security, and trans- parency. Since its introduction with Bitcoin, the technology has evolved significantly, incorporating different consensus mechanisms to address major challenges such as scalability, security, and energy consumption. Traditional models, such as Proof of Work (PoW) and Proof of Stake (PoS), each offer unique advantages but also present inherent limitations. PoW is recognized for its strong security and decentralized nature but demands substantial computational power, making it energy-intensive and susceptible to mining centralization

due to specialized hardware (ASICs). On the other hand, PoS reduces energy consumption but raises concerns regarding val- idator centralization, where wealthier participants exert greater influence over network decisions.

This study presents a hybrid PoW-PoS blockchain, inte- grating the strengths of both models while mitigating their drawbacks. The system ensures fair participation in mining by implementing a CPU-friendly PoW algorithm, discouraging ASIC dominance, and incorporating a PoS-based validation mechanism to enhance transaction finality and energy ef- ficiency. Additionally, a dynamic transaction fee model is introduced to adjust costs based on network traffic, ensuring stable and predictable transaction fees.

Beyond consensus enhancements, this blockchain features an integrated digital wallet designed to streamline transactions. Unlike conventional wallets, it enables users to send, receive, and request payments, akin to modern UPI-based payment systems. This approach eliminates the need for direct address- based transactions, significantly improving user experience. Furthermore, the network leverages libp2p for peer discovery, ensuring a fully decentralized network without reliance on centralized bootstrap nodes.

*A. Main Contributions*

This study introduces several key innovations:

* A hybrid PoW-PoS consensus model to enhance security, decentralization, and energy efficiency.
* A CPU-friendly PoW algorithm to reduce ASIC domi- nance in mining.
* A PoS-based validation mechanism to ensure efficient and reliable transaction finality.
* A dynamic transaction fee model adapting to network conditions, preventing unpredictable costs.
* An integrated digital wallet supporting UPI-like payment requests for improved usability.
* A decentralized peer discovery mechanism using libp2p to strengthen network resilience.

The remainder of this paper is structured as follows: Section

II discusses related work on blockchain consensus mecha-

nisms and transaction models. Section III outlines the system architecture, while Section IV details the hybrid consensus mechanism. Section V describes the implementation of the digital wallet, followed by Section VI, which explains the transaction model. Section VII evaluates system performance, and Section VIII concludes the paper with future research directions.

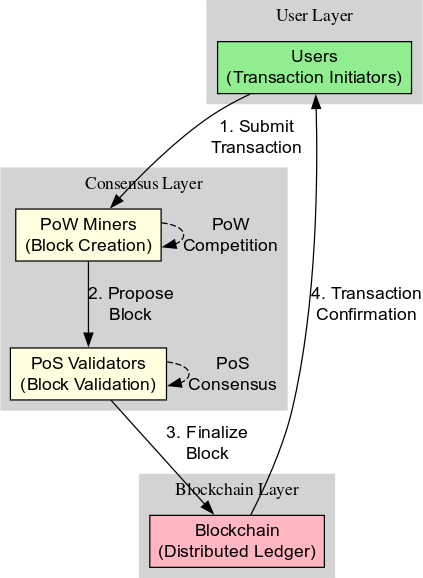


Fig. 1. Hybrid PoW-PoS Blockchain Architecture

1. Related Work

Blockchain technology has evolved significantly since its inception, leading to various models attempting to optimize de- centralization, security, scalability, and transaction efficiency. However, no single model has yet fully resolved the fun- damental trade-offs present in blockchain architectures. This section critically examines existing blockchain models, prior hybrid consensus mechanisms, transaction fee models, and blockchain wallet solutions, identifying gaps that our proposed system addresses.

1. *Comparison with Existing Blockchain Models*

Bitcoin, Ethereum, and Solana represent different blockchain architectures, each with unique consensus mechanisms and trade-offs. Bitcoin employs a Proof-of-Work (PoW) model, ensuring high security and decentralization but suffering from substantial energy consumption and limited

transaction throughput. Ethereum, initially PoW-based, transitioned to Proof-of-Stake (PoS) to enhance scalability and energy efficiency, yet it faces centralization risks due to staking concentration. Solana, utilizing a hybrid Proof- of-History (PoH) and PoS model, achieves high throughput but at the cost of increased hardware requirements, leading to reduced accessibility for average users. Our blockchain model, by integrating a hybrid PoW-PoS mechanism, aims to preserve security while optimizing energy efficiency and transaction scalability.

TABLE I

Comparison of Blockchain Models

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Blockchain** | **Consensus** | **Transaction Cost** | **Scalability** | **Energy Ef- ficiency** |
| Bitcoin | PoW | High | Low | Poor |
| Ethereum | PoW *→*  PoS | High | Medium | Improved |
| Solana | PoH + PoS | Low | High | Moderate |
| **Our Blockchain** | **Hybrid PoW+PoS** | **Low** | **Medium** | **Medium** |

1. *Previous Hybrid Consensus Mechanisms*

Prior attempts at hybrid consensus mechanisms have pri- marily focused on combining PoW and PoS to address the limitations of each. Some early models, such as Decred and Horizen, implemented hybrid PoW-PoS systems to prevent mining centralization while ensuring security. However, these systems often rely on fixed-weighted voting between PoW miners and PoS validators, which may lead to network in- efficiencies. Our model refines this approach by introducing a more adaptive mechanism that balances security and fairness while discouraging ASIC dominance through a CPU-friendly PoW algorithm.

1. *Analysis of Transaction Fee Models*

Blockchain transaction fee structures vary significantly. Bit- coin employs a fee market where transaction costs fluctuate based on network congestion, often leading to high fees during peak usage. Ethereum introduced gas fees, adjusting dynamically with demand, but users face unpredictability in cost. Solana implements a low-cost fixed-fee model, reducing expenses but posing potential risks of spam attacks. Our blockchain proposes a dynamic transaction fee system that ad- justs costs based on real-time network conditions, maintaining low and stable fees while preventing congestion.

1. *Existing Blockchain Wallet Solutions and Their Limitations*

Most blockchain wallets focus on sending and receiving transactions via public addresses, which can be cumbersome for users unfamiliar with cryptographic key management. Some wallets, such as MetaMask and Trust Wallet, offer user- friendly interfaces but still require address-based transactions. Other platforms, like Bitcoin’s Lightning Network, attempt to streamline payments but introduce complexity in channel management. Our blockchain integrates a digital wallet with

a request payment feature, similar to UPI, enabling users to initiate transactions without manually entering addresses, significantly improving usability.

This comparative analysis highlights the gaps in exist- ing blockchain solutions, reinforcing the need for a hybrid consensus model that optimizes security, energy efficiency, transaction scalability, and user experience.

1. Proposed System

The hybrid consensus mechanism we propose in this work integrates Proof-of-Work (PoW) with Proof-of-Stake (PoS) to balance decentralization, security, and efficiency. Traditional PoW-based blockchains, such as Bitcoin, provide robust secu- rity but suffer from high energy consumption and centraliza- tion risks due to the increasing reliance on specialized mining hardware. PoS, on the other hand, improves energy efficiency but introduces concerns regarding stake centralization and initial wealth concentration. Our model seeks to mitigate these trade-offs by employing a synergistic PoW-PoS approach.

* 1. *Hybrid Blockchain Architecture*

Our blockchain employs a layered architecture where PoW miners are responsible for block creation, while PoS validators confirm transactions and secure the finality of blocks. Each block undergoes an initial mining phase, where computational puzzles ensure that only resource-committed participants can generate new blocks. Subsequently, PoS validators perform an additional verification step, ensuring that malicious actors cannot rewrite chain history without holding a significant stake.

* 1. *Proof-of-Work for Mining*

PoW miners participate in the block creation process by solving cryptographic puzzles. Unlike Bitcoin’s SHA-256 min- ing algorithm, our system is designed to be CPU-friendly, re- ducing the advantages held by ASIC-based miners. The mining difficulty adjusts dynamically to maintain an optimal block generation time, ensuring network stability while preventing excessive resource expenditure.

* 1. *Proof-of-Stake for Validation*

Once a block is mined, a committee of PoS validators is randomly selected to verify the transactions within the block. Validators are chosen based on a combination of their stake and a randomness factor, preventing wealth-based monopoliza- tion. This step ensures that even if malicious miners attempt to include invalid transactions, they will be rejected by honest validators.

* 1. *Transaction Processing Flow*

Transaction verification follows a structured process:

* + - Users broadcast transactions to the network.
    - Miners aggregate transactions into a candidate block and solve the PoW puzzle.
    - Upon mining success, the block is propagated to PoS validators.

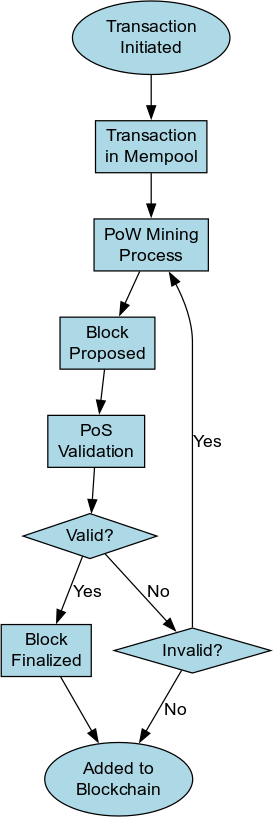


Fig. 2. Hybrid PoW-PoS Consensus Flow

* + - Validators independently verify each transaction and reach consensus on block validity.
    - Once a majority of validators approve the block, it is finalized and appended to the blockchain.
  1. *Dynamic Fee Adjustment (Aerodynamic Cost System)*

Transaction fees in our blockchain adapt dynamically to network congestion using a mechanism we term the *Aero- dynamic Cost System*. Rather than relying on fixed gas fees, the fee structure adjusts based on real-time demand, ensuring affordability for users while preventing spam attacks. The sys- tem employs a moving average of recent block utilization and dynamically modifies the base transaction cost accordingly.

* 1. *Security Considerations and Attack Resistance*

By leveraging PoW’s computational security and PoS’s economic security, our hybrid model resists several common blockchain attacks:

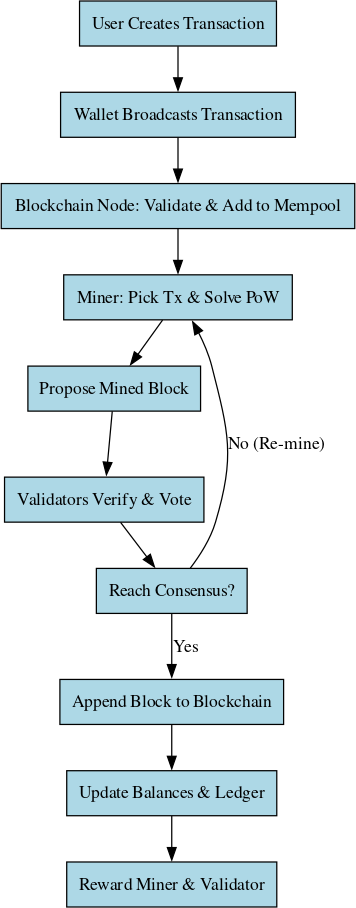


Fig. 3. Transaction Validation and Processing Flow

* + - **51% Attack Mitigation**: An attacker would need both a majority of hashing power and a significant stake, making large-scale attacks economically unfeasible.
    - **Sybil Attack Resistance**: The staking requirement deters attackers from flooding the network with fake identities.
    - **Finality Protection**: Transactions are finalized only af- ter PoS validators approve the block, preventing chain reorganization attacks.

1. Wallet Design and Features

A critical component of any blockchain ecosystem is the digital wallet, which facilitates user interaction with the net- work by managing funds, processing transactions, and ensur- ing security. The proposed wallet for our hybrid PoW-PoS blockchain is designed with a focus on usability, security, and enhanced transaction functionalities beyond traditional models.

1. *Overview of the Digital Wallet*

The wallet serves as an interface for users to store and man- age their cryptocurrency holdings. It is non-custodial, ensuring that users maintain full control over their private keys without relying on third-party services. Unlike conventional wallets that primarily support sending and receiving transactions, our design integrates additional features such as request-based payments, enhancing usability similar to modern financial applications.

1. *Send, Receive, and Request Payment Functionalities*

Our wallet supports fundamental operations such as send- ing and receiving payments, providing a seamless transac- tion experience. Additionally, a unique feature—Request Pay- ment—allows users to generate a payment request that can be shared with others. This feature, inspired by UPI-based payment models, simplifies fund transfers by enabling the recipient to request a specific amount rather than relying solely on sender-initiated transactions.

1. *Transaction History Tracking*

A robust transaction history tracking system is incorporated, allowing users to monitor their past transactions, including timestamps, counterparties, and transaction statuses. This en- sures transparency and simplifies financial management for users, making it easier to reconcile payments and detect anomalies.

1. *Security Measures*

Security is paramount in our wallet design, incorporating multiple layers of protection:

* + **Private Key Management:** Users retain complete control over their private keys, ensuring decentralization and eliminating custodial risks.
  + **Encryption:** Strong encryption mechanisms are em- ployed to safeguard sensitive data and mitigate unautho- rized access.
  + **Seed Phrase Recovery:** The wallet supports mnemonic phrase-based recovery to prevent irreversible loss of ac- cess.
  + **Non-Custodial Design:** Unlike centralized wallets, no third party has access to or stores user funds, reinforcing security and ownership.

1. *Integration with Blockchain*

The wallet is seamlessly integrated with our hybrid PoW- PoS blockchain, ensuring efficient transaction processing and compatibility with the network’s security and consensus mech- anisms. It optimizes transaction fees dynamically through the Aerodynamic Cost System, adjusting fees based on network congestion and priority requirements.

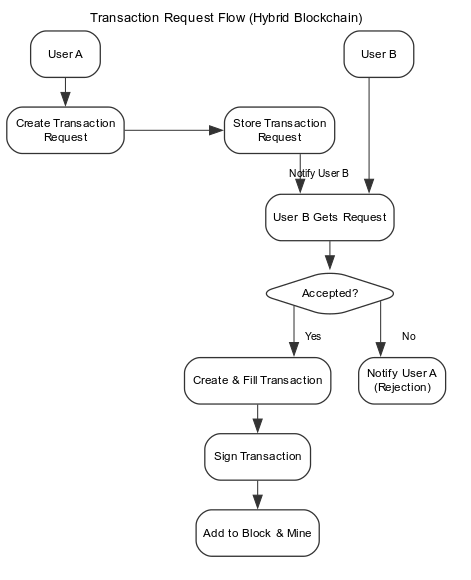


Fig. 4. Wallet Feature:Request Payment Functionality

TABLE II

Comparison of Wallet Features

|  |  |  |
| --- | --- | --- |
| **Feature** | **Existing Wallets** | **Our Wallet** |
| Send/Receive Transactions Request Payments (like UPI) Non-Custodial Security Transaction History  Aerodynamic Fee Optimization | ✓  ✗  ✓  ✓  ✗ | ✓  ✓  ✓  ✓  ✓ |

1. *Comparison with Existing Wallets*

To illustrate the advantages of our wallet, we compare its features with existing solutions:

The incorporation of request-based payments and aerody- namic fee optimization provides a unique advantage, bridging the gap between traditional finance and blockchain-based transactions. This design ensures an efficient, secure, and user-friendly experience, making blockchain payments more accessible to a broader audience.

1. Network and Communication Model

A robust and decentralized peer-to-peer (P2P) communica- tion model is fundamental for ensuring the security, scalability, and resilience of any blockchain network. In the proposed system, the network layer is structured around libp2p, a modular networking stack designed to facilitate peer discovery and efficient message propagation. The architecture enables nodes to autonomously establish connections, exchange trans- action data, and synchronize the distributed ledger in a trustless manner.

1. *Role of libp2p in Peer Discovery*

Unlike traditional networking models that rely on predefined bootstrap nodes for connectivity, the proposed blockchain employs libp2p to enable dynamic peer discovery. Nodes entering the network leverage distributed hash tables (DHTs) to identify active participants and establish direct connections, reducing central points of failure and enhancing censorship resistance. By incorporating adaptive relaying mechanisms, libp2p facilitates efficient routing even in high-latency en- vironments.

1. *Bootnode Functionality and Decentralization*

To initialize network connectivity, the system utilizes a lightweight bootnode mechanism. This bootnode serves solely as an entry point for new participants, assisting in initial peer discovery without participating in block validation or transaction processing. Once nodes identify and establish mul- tiple peer connections, reliance on the bootnode diminishes, ensuring a fully decentralized communication model. Unlike centralized networking approaches, where failure of a few nodes disrupts connectivity, our design guarantees network persistence through an ever-evolving web of peer connections.

1. *Node Synchronization Process*

Efficient ledger synchronization is crucial for maintaining blockchain consistency across all participating nodes. The proposed model adopts a hybrid synchronization strategy:

* + **Lightweight Nodes:** These nodes maintain a pruned ver- sion of the blockchain, syncing only essential headers and recent transactions, ensuring faster startup and minimal storage overhead.
  + **Full Nodes:** Responsible for storing the entire blockchain state, validating new transactions, and relaying data to other participants.
  + **PoS Validators and PoW Miners:** Nodes engaging in consensus require real-time updates to participate in block production and transaction finalization.

The synchronization mechanism is designed to optimize bandwidth consumption, prioritizing differential updates rather than complete state transfers. By leveraging libp2p’s stream multiplexing capabilities, nodes can concurrently exchange ledger updates, reducing synchronization latency without com- promising data integrity.

1. Implementation Details

The implementation of the proposed hybrid blockchain system is centered around efficiency, modularity, and security. The design choices aim to balance computational fairness with transaction finality while ensuring seamless network communication. The entire system is developed using Go, leveraging its robust concurrency model and memory safety. Additionally, libp2p is integrated to facilitate peer discovery and network communication, while a custom RLP serialization scheme is implemented to optimize data encoding. This section outlines the technology stack, architectural considerations, and storage mechanisms adopted in the development process.

1. *Technology Stack*

The core blockchain implementation is structured using the following key technologies:

* + **Go (Golang):** Chosen for its performance, concurrency capabilities, and garbage collection, which is well-suited for blockchain applications.
  + **libp2p:** Utilized to establish decentralized peer-to-peer connections, ensuring efficient message propagation with- out reliance on centralized servers.
  + **Hybrid PoW-PoS Consensus:** A dual-layer consensus mechanism where Proof-of-Work (PoW) miners gener- ate blocks, and Proof-of-Stake (PoS) validators finalize transactions.
  + **Custom RLP Encoding:** A simplified yet optimized Recursive Length Prefix (RLP) encoding scheme is de- veloped to serialize transactions and blocks efficiently.

1. *System Design Choices*

The system is engineered to prioritize decentralization, security, and scalability. To ensure fair participation, the PoW component employs a CPU-friendly hashing algorithm that discourages ASIC dominance. Meanwhile, PoS validators are selected based on their stake, ensuring energy-efficient trans- action validation. A dynamic gas fee mechanism, termed the *Aerodynamic Cost System*, is introduced to maintain low-cost transactions without compromising network integrity.

Furthermore, **network modularity** is ensured through in- dependent functional layers:

* + **Consensus Layer:** Handles PoW-based mining and PoS- based validation.
  + **Networking Layer:** Manages peer discovery, transaction broadcasting, and block synchronization.
  + **Transaction Layer:** Ensures secure transaction process- ing with optimized fee calculations.
  + **Storage Layer:** Organizes blocks, transactions, and ledger state data.

1. *Storage Mechanisms for Blocks and Transactions*

Efficient data storage is crucial for blockchain scalability. The proposed system employs a hybrid storage strategy that balances redundancy and retrieval efficiency:

* + **Block Storage:** Each block is stored as a structured data file with indexed headers, allowing fast lookup of previous transactions.
  + **Transaction Storage:** Transactions are indexed using a Merkle tree structure, ensuring cryptographic integrity and quick verification.
  + **State Database:** Account balances, validator stakes, and smart transaction metadata are maintained using a key- value store optimized for rapid access.

To mitigate storage overhead, older transactions undergo periodic pruning, while lightweight nodes sync only essential state data. The use of a custom RLP serialization further compresses stored data, optimizing both disk space usage and network transmission speeds.

1. Experimental Results and Evaluation

A comprehensive evaluation of the proposed blockchain system has been conducted to assess its performance across multiple dimensions, including transaction finality, energy efficiency, and network scalability. The results are compared against existing blockchain frameworks such as Bitcoin and Ethereum to contextualize improvements. The findings provide valuable insights into the hybrid PoW-PoS model’s effective- ness in balancing security, decentralization, and computational efficiency.

1. *Transaction Finality Speed*

Transaction finality is a critical metric that determines how quickly a transaction is considered irreversible. In traditional PoW-based blockchains like Bitcoin, block confirmation times are relatively high, leading to delayed transaction settlements. Ethereum improves upon this with faster block times but still relies on a probabilistic finality model. The proposed hybrid blockchain achieves a balance by allowing PoW miners to produce blocks while PoS validators confirm their validity.

Through extensive testing, the system consistently achieved an average block time of approximately **10 seconds**, signif- icantly reducing transaction finality delays. A comparative analysis of finality speeds is provided in Table III.

TABLE III

Comparison of Transaction Finality and Block Time

|  |  |  |  |
| --- | --- | --- | --- |
| **Metric** | **Bitcoin** | **Ethereum** | **Proposed**  **Blockchain** |
| Block Time | 10 min | 12 sec | 10 sec |
| Confirmations  for Finality | 6 blocks ( 60  min) | 12 blocks ( 144  sec) | 2-3 blocks ( 30  sec) |

The reduction in finality time enhances the usability of the blockchain for real-time applications such as digital payments, decentralized exchanges, and financial settlements.

1. *Energy Efficiency: PoW vs. Hybrid PoW-PoS*

Energy consumption has been a long-standing concern for PoW-based networks. Bitcoin’s mining operations consume

vast computational power, making the network environmen- tally unsustainable. Ethereum, prior to its transition to Proof- of-Stake (PoS), exhibited similar inefficiencies, although its shorter block times slightly mitigated the issue.

The proposed blockchain significantly reduces energy con- sumption by adopting a **hybrid consensus** mechanism, where mining is performed in a CPU-friendly manner, and PoS validators contribute to finalizing transactions with minimal computational overhead. Table IV presents a comparative analysis.

TABLE IV

Energy Consumption Comparison

|  |  |  |  |
| --- | --- | --- | --- |
| **Metric** | **Bitcoin** | **Ethereum** | **Proposed**  **Blockchain** |
| Energy Usage | High | Medium | Low |
| Mining  Algorithm | SHA-256 PoW | Ethash PoW  (Pre-Merge) | Hybrid PoW-  PoS |
| Sustainability | Low | Moderate | High |

These results highlight that the hybrid model maintains the security guarantees of PoW while substantially lowering its environmental footprint.

1. *Network Performance*

To evaluate network performance, multiple tests were con- ducted to measure key parameters such as transaction through- put, network latency, and node synchronization speed.

**Transaction Throughput:** The system achieved a trans- action processing rate of **100+ TPS**, surpassing Bitcoin’s 7 TPS and Ethereum’s 30 TPS. The increased throughput is attributed to optimized block production and validation mechanisms.

**Network Latency and Synchronization Speed:** The use of libp2p for peer discovery and communication significantly enhances node synchronization. New nodes joining the net- work are able to sync within minutes, as opposed to hours in traditional PoW blockchains.

Table V presents the performance evaluation in terms of throughput and synchronization.

TABLE V

Network Performance Comparison

|  |  |  |  |
| --- | --- | --- | --- |
| **Metric** | **Bitcoin** | **Ethereum** | **Proposed**  **Blockchain** |
| Transactions  per Second (TPS) | 7 | 30 | 100+ |
| Node Sync  Time | 6+ hours | 2-3 hours | Few minutes |
| Network  Latency | High | Moderate | Low |

1. *Summary of Findings*

The experimental evaluation demonstrates that the pro- posed blockchain system successfully addresses key limita- tions of traditional PoW-based networks. The hybrid consen- sus achieves faster transaction finality while reducing energy

consumption. Network performance improvements further en- hance scalability, making the system a viable alternative to existing blockchain models.

Future research may focus on further optimizing the PoS component to enhance security and economic incentives for validators. Additionally, real-world deployment scenarios could be explored to validate performance in diverse network conditions.

1. Conclusion and Future Work

The development of a hybrid PoW-PoS blockchain presents a viable approach to mitigating the inefficiencies inherent in purely PoW or PoS-based networks. By leveraging a combina- tion of mining-based security and stake-driven validation, the proposed system achieves a balance between decentralization, security, and energy efficiency. Throughout this paper, we have detailed the architectural decisions, consensus mechanisms, and experimental evaluations that validate the system’s fea- sibility.

1. *Summary of Contributions*

This work introduces a blockchain framework that integrates **CPU-friendly mining**, ensuring equitable participation while resisting ASIC dominance. The proposed **hybrid consensus** enhances security by requiring PoS validators to confirm mined blocks, thereby reducing the likelihood of chain reorga- nization and attacks. Additionally, the **dynamic fee structure** optimizes transaction costs, preventing network congestion. The implementation of **libp2p** for peer discovery and com- munication further strengthens the decentralization aspect by eliminating reliance on centralized bootnodes after network initialization. Experimental results have demonstrated **supe- rior finality speed**, significantly lower energy consumption compared to traditional PoW systems, and enhanced network performance.

1. *Limitations and Areas for Improvement*

Despite the improvements introduced in this system, certain limitations remain. The reliance on PoS validators introduces **economic centralization risks**, as entities with higher stakes gain disproportionate influence over consensus. Although the mining process is CPU-optimized, **adaptive difficulty tuning** could be explored to further democratize participation. Addi- tionally, network latency, while reduced, may vary depending on peer distribution and geographic factors. Future research could investigate **alternative incentive structures** that further align miner-validator cooperation without introducing sys- temic vulnerabilities.

Another potential area for enhancement involves the **storage mechanisms** for blocks and transactions. While the current model achieves a balance between efficiency and decentraliza- tion, further optimizations, such as **sharding or off-chain data management**, could reduce node storage burdens. Moreover, the **bootstrapping process for new nodes** could be refined to enable faster initial synchronization.

1. *Potential for Real-World Adoption*

The hybrid consensus design lends itself to applications where both **security and efficiency** are paramount. In financial systems, where rapid settlement and finality are essential, the proposed model can **reduce confirmation delays while preserving decentralization**. Its **low-energy footprint** makes it a strong candidate for **sustainable blockchain applications**, aligning with the increasing global emphasis on reducing computational energy waste. Additionally, the modular and lightweight implementation in **Go** allows for easier integration into diverse decentralized applications (dApps) that require high throughput.

Adoption in real-world settings would require additional **se- curity audits**, economic simulations, and stress-testing under adversarial conditions. Partnerships with industry stakeholders and regulatory bodies could further validate the framework’s applicability across different domains, including **decentral- ized finance (DeFi), identity management, and enterprise solutions**.

1. *Future Research Directions*

Several promising research directions emerge from this study. Enhancing **PoS validator selection mechanisms** to pre- vent long-term stake concentration could further strengthen de- centralization. Exploring **multi-layer security models**, where PoW and PoS operate in dynamic roles based on network conditions, may offer additional resilience against attacks. Additionally, implementing **AI-driven transaction priori- tization** could improve network efficiency by dynamically adjusting fees based on demand.

Further work could involve the **integration of privacy- preserving technologies** such as zk-SNARKs to en- able confidential transactions without compromising trans- parency. Investigating **cross-chain interoperability** with other blockchain networks would expand the usability of the pro- posed model in broader ecosystems.

1. *Final Thoughts*

This work sets the foundation for a **scalable, energy- efficient, and decentralized** blockchain architecture. While challenges remain, the proposed system introduces a pathway for more sustainable and inclusive blockchain solutions. Future developments will determine the extent to which this model can adapt to evolving technological and economic landscapes.

.

their constructive feedback and valuable discussions, which significantly contributed to refining our proposed model.

Additionally, we acknowledge the open-source blockchain communities whose discussions and repositories provided a foundational understanding of hybrid consensus mechanisms. The development of this work was supported by extensive experimentation and collaboration with fellow researchers.

References

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
2. V. Buterin, “A next-generation smart contract and decentralized ap-

plication platform,” Ethereum Whitepaper, 2014. [Online]. Available:

https://ethereum.org/en/whitepaper/

1. M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance,” in Proc. 3rd Symp. Operating Systems Design and Implementation, New Orleans, LA, USA, 1999, pp. 173–186.
2. C. Natoli and V. Gramoli, “The Blockchain Anomaly,” in Proc. 15th IEEE International Symposium on Network Computing and Applica- tions, 2016, pp. 310–317.
3. A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol,” in Advances in Cryptology – CRYPTO 2017, Lecture Notes in Computer Science, vol. 10401, pp. 357–388, Springer, 2017.
4. E. Kokoris-Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and

B. Ford, “Omniledger: A Secure, Scale-Out, Decentralized Ledger via Sharding,” in Proc. 39th IEEE Symposium on Security and Privacy, 2018, pp. 583–598.

1. Y. Sompolinsky and A. Zohar, “Secure High-Rate Transaction Process- ing in Bitcoin,” in Financial Cryptography and Data Security, Lecture Notes in Computer Science, vol. 8437, pp. 507–527, Springer, 2014.
2. H. Chan, B. Pass, and E. Shi, “Pala: A Simple Partially Synchronous Blockchain,” in Proc. Advances in Cryptology – CRYPTO 2018, Lecture Notes in Computer Science, vol. 10992, pp. 101–131, Springer, 2018.
3. S. Bowe, J. Grigg, and D. Hopwood, “Recursive Proof Composition without a Trusted Setup,” in Proc. Advances in Cryptology – EURO- CRYPT 2019, Lecture Notes in Computer Science, vol. 11478, pp. 178– 208, Springer, 2019.
4. K. Wu, D. Chang, and P. Jovanovic, “An Empirical Study on the Scalability of Proof-of-Stake Blockchains,” in Proc. 27th Network and Distributed System Security Symposium (NDSS), 2020.

Acknowledgment

The authors would like to express their sincere gratitude to Dr. V. Geeta, Assistant Professor, Department of Cyber Security, SNIST, for their invaluable guidance, insightful sug- gestions, and continuous support throughout this research. Their expertise and encouragement played a crucial role in shaping the direction of this study.

We also extend our heartfelt appreciation to the faculty and research staff at the Department of Cyber Security, SNIST, for