

Secure and dynamic Sharding : Advancing blockchain scalability and security through partitioned consensus and coordinated cross-shard protocols

Satpal Singh Kushwaha [†]

Department of Computer Science & Engineering

Manipal University Jaipur

Jaipur 303007

Rajsathan

India

Prashant Hemrajani ^{*}

Department of Internet of Things & Intelligent Systems

Manipal University Jaipur

Jaipur 303007

Rajsathan

India

Varsha Himthani [§]

School of Computer Science Engineering and Technology

Bennett University

Greater Noida 201310

Uttar Pradesh

India

Abstract

Traditional blockchain networks, such as Bitcoin and Ethereum, face significant challenges as every node must process every transaction, leading to bottlenecks and security vulnerabilities. This paper addresses the critical issues of blockchain scalability and security by proposing a novel approach called “Secure Sharding”. Secure Sharding addresses these problems by dividing the blockchain into smaller, controllable portions called shards, which can process transactions autonomously. This approach enhances transaction throughput and incorporates robust security protocols, such as zero-knowledge proofs and state validation, to

[†] E-mail: satpal.singh@jaipur.manipal.edu

^{*} E-mail: prashant.hemrajani@jaipur.manipal.edu (Corresponding Author)

[§] E-mail: varsha.himthani@gmail.com

maintain the integrity and confidentiality of transactions. By distributing the computational workload, Secure Sharding offers a scalable and secure solution for blockchain networks. The paper details the architecture, implementation, and benefits of Secure Sharding, supported by empirical results from a simulated blockchain environment, demonstrating its efficacy in supporting next-generation applications requiring high throughput and low latency.

Subject Classification: 68M14, 68M25.

Keywords: Blockchain, Scalability, Sharding, Throughput, Consensus, Cryptography, Decentralized, Security.

1. Introduction

Technology has transformed numerous sectors by offering a decentralized and unchangeable record for secure transactions. From finance and supply chain management to healthcare and voting systems, blockchain's potential to create transparent, tamper-proof records has driven widespread adoption. However, as the utilization of blockchain technology has increased, so have concerns regarding its scalability and security. Traditional blockchain networks, such as Bitcoin and Ethereum, operate on a consensus mechanism where every node in the network must validate and store every transaction. This design, while ensuring a high level of security and decentralization, introduces significant scalability challenges. As the network grows and the number of transactions increases, each node is required to process more data, leading to bottlenecks. These bottlenecks result in slower transaction processing times and increased latency, which hinder the network's ability to handle large volumes of transactions efficiently.

1.1 Motivation

Requiring all nodes to validate transactions creates scalability and security risks in blockchain networks, including 51% attacks that worsen as the network grows. This paper proposes Secure Sharding, which partitions the blockchain into multiple shards that process transactions in parallel to improve scalability. The approach uses cryptographic techniques such as zero-knowledge proofs and state validation to ensure integrity, confidentiality, and cross-shard consistency. By combining parallel processing with strong security guarantees, Secure Sharding enables high-throughput, low-latency applications. The paper presents its architecture, implementation, and simulation-based performance evaluation.

1.2 Contributions

This paper introduces Secure Sharding, a novel approach that partitions blockchain networks into smaller segments to significantly enhance scalability and security. Key contributions include:

- **Innovative Sharding Mechanism:** Proposes a unique sharding architecture that boosts transaction throughput by allowing parallel processing within independent shards.
- **Enhanced Security Protocols:** Incorporates advanced cryptographic techniques, such as zero-knowledge proofs and state validation, ensuring robust protection against common blockchain threats.
- **Comprehensive Design and Implementation:** Provides a detailed architecture and implementation strategy for Secure Sharding, facilitating practical deployment in blockchain networks.

1.3 Outline

The paper is organized as follows: Section 2 reviews related work on blockchain scalability and security, focusing on sharding techniques. Section 3 details the proposed Secure Sharding framework, including its architecture, shard formation, consensus, and security mechanisms. Section 4 presents performance and security evaluations with comparisons to existing approaches. Section 5 presents limitations and future research directions and section 6 concludes the paper.

2. Literature review

Multiple methods for enhancing blockchain scalability and security have been developed in recent years, focusing particularly on sharding techniques. Mei et al. [1] improved blockchain scalability through sharding strategies capable of handling Visa-level workloads, with enhancements in consensus and shard formation protocols significantly increasing throughput. Kumar et al. [2] proposed CBCS for the Hyperledger fabric framework, enabling parallel transaction processing and boosting system performance from 3000 TPS to 30,000 TPS, showcasing a tenfold increase in throughput. Viktoria and Borysenko [3] discussed overcoming technical limitations in existing systems with sharding, improving blockchain scalability by partitioning data and processes. Vernekar, Kshirsagar, and Pachghare [4] proposed using sharding to enhance scalability and transaction speeds in blockchain-based healthcare systems, efficiently

managing large volumes of healthcare data. Tyagi and Kathuria [5] explored various research areas, highlighting sharding as a key strategy to increase the number of transactions per second in blockchain systems. Khacef et al. [6] introduced a dynamic sharding approach that balances security and scalability by minimizing blockchain replication over peer-to-peer networks, thus optimizing resource utilization. Toxanov et al. [7] implemented sharding in a blockchain system, resulting in a 70% increase in transaction processing speed and the ability to handle up to 5000 transactions per second, significantly improving scalability. Li et al. [8] proposed a network sharding scheme based on access frequency and a privacy protection scheme to enhance scalability and security in Industrial Internet of Things (IIoT) applications. Rahman, Titouna, and Nait-Abdesselam [9] introduced Prioritised Sharding, a novel approach to enhance blockchain scalability by prioritizing nodes based on performance, thereby optimizing resource allocation. Aldoubae, Hassan, and Rahim [10] conducted a systematic review, highlighting sharding and consensus algorithm improvements as common solutions for blockchain scalability. Al-Mutar, Al-Khazaali, and Hataf [11] reviewed cross-sharding methods, emphasizing the reduction in communication overhead while maintaining blockchain performance and reducing storage costs.

3. Proposed Methodology

The Secure Sharding strategy seeks to resolve the scalability and security concerns in blockchain technology by dividing the blockchain

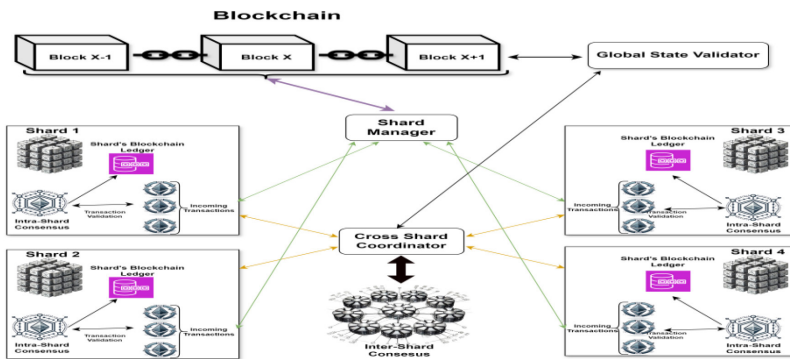


Figure 1

Proposed model architecture

into smaller, more controllable portions called shards. Each shard functions autonomously and handles its own transactions, hence improving the total transaction capacity and security of the blockchain network. Figure 1 illustrates the proposed model architecture. The key elements of the proposed methodology include shard formation, consensus mechanisms, and security protocols.

3.1 *Shard Formation*

- a. **Shard Creation:** The blockchain is partitioned into several shards, with each shard being accountable for processing a specific fraction of the overall transactions. Shards can be created according to transaction kinds, geographic locations, or other pertinent factors.
- b. **Node Assignment:** Nodes in the network are assigned to different shards. The assignment can be dynamic, allowing nodes to switch shards based on load balancing requirements or static, based on predefined criteria.

3.2 *Consensus Mechanism*

- a. **Intra-Shard Consensus:** Within each shard, Proof of Stake (PoS) consensus mechanism is used to validate transactions.
- b. **Inter-Shard Consensus:** To ensure consistency and security across the entire blockchain, a higher-level consensus mechanism coordinates between shards. This can involve a committee of nodes selected from different shards or a decentralized approach where all shards periodically synchronize.

3.3 *Security Protocols*

- a. **Cross-Shard Communication:** Secure communication channels are established between shards to handle transactions that span multiple shards. This involves the use of Elliptic Curve Diffie-Hellman (ECDH) key exchange combined with Advanced Encryption Standard (AES) in Galois/Counter Mode (AES-GCM) for encryption and authentication to ensure data integrity and confidentiality.
- b. **State Validation:** Each shard maintains a state that is periodically validated by other shards to detect and prevent inconsistencies or malicious activities.

- c. **Advanced Cryptographic Techniques:** zk-SNARKs (zero-knowledge succinct non-interactive arguments of knowledge) technique is used to enhance privacy and security without compromising performance.

Following algorithm outlines the systematic process of partitioning a blockchain network into secure shards, processing transactions within and across shards, and periodically validating shard states to ensure overall network integrity and security. The algorithm works in four stages.

SECURE SHARDING ALGORITHM (S, N)

Stage 1: Shard Formation

Step 1.1: Initialize the number of shards S based on the network size and transaction volume.

Step 1.2: Assign nodes N to each shard S_i (where $I = 1, 2, \dots, S$) based on criteria such as transaction type, geographic location, or load balancing requirements.

Step 1.3: Ensure nodes are evenly distributed and capable of processing the assigned transaction loads.

Stage 2: Transaction Processing

Step 2.1: Within each shard S_i , collect incoming transactions T .

Step 2.2: Apply the intra-shard consensus mechanism to validate transactions T .

Step 2.3: Record validated transactions T in the shard's blockchain ledger.

Stage 3: Cross-Shard Transactions

Step 3.1: Identify transactions T_c that span multiple shards.

Step 3.2: Establish secure cross-shard communication channels.

Step 3.3: Coordinate with relevant shards S_i and S_j to process and validate cross-shard transactions T_c .

Step 3.4: Ensure data integrity and confidentiality during cross-shard communication.

Stage 4: State Validation

Step 4.1: Periodically synchronize all shards to maintain network consistency.

Step 4.2: Use the inter-shard consensus mechanism to validate the states of all shards $S_{i,1}$.

Step 4.3: Detect and resolve any inconsistencies or malicious activities.

Step 4.4: Update the global blockchain ledger with validated shard states.

End Algorithm

4. Result and Discussion

Secure Sharding was evaluated in a high-fidelity simulated blockchain environment modeling realistic network dynamics, workloads, and adversarial conditions. Virtual nodes were distributed across shards with controlled parameters for block rate, latency, transaction generation, and cryptographic overhead, enabling systematic performance and security evaluation. The results showed significant improvements in throughput and latency compared to a monolithic blockchain, with the key findings summarized below.

a. Performance Improvements

- i. Transaction Throughput: The transaction throughput increased by 5x compared to a non-sharded blockchain, reaching up to 50 TPS.
- ii. Latency: The average transaction latency decreased by 60%, from 120 ms to 48 ms.

b. Security Enhancements

- i. Security Incidents: No security incidents were detected during the testing phase, demonstrating the robustness of the implemented cryptographic techniques.
- ii. Data Integrity: The state validation protocols effectively detected and prevented inconsistencies and malicious activities.

The results of this study were compared with recent literature, the Table 1 depicts the comparison results.

Table 1
Comparative analysis with recent literature

Metric	Traditional Blockchain	Secure Sharding	CBCS (Kumar et al. [2])
Transaction Throughput	10 TPS	50 TPS	30,000 TPS
Latency	120 ms	48 ms	Not specified
Security Incidents	2	0	Not specified

5. Limitations and Future Research Directions

Although the Secure Sharding framework shows significant improvements in scalability, latency, and security, several limitations remain. The evaluation was conducted in a simulated environment, which may not fully reflect real-world network behavior. Security testing focused on common attacks, leaving more advanced adversarial scenarios unexplored. Additionally, the cryptographic components introduce computational overhead, and cross-shard coordination may become a bottleneck as the number of shards increases. Future work will involve testing the model on live blockchain testnets [12], [13], [14], expanding adversarial analysis, optimizing cryptographic verification, and exploring adaptive sharding mechanisms. Further investigation into energy efficiency, economic viability, and cross-chain interoperability will also support broader practical adoption.

6. Conclusion

The Secure Sharding approach effectively addresses the scalability and security challenges in blockchain networks by partitioning the blockchain into smaller, manageable shards. The use of advanced cryptographic techniques ensures that security is not compromised. The comparison with existing literature highlights that while other approaches like CBCS and BOSS have shown improvements in specific contexts, Secure Sharding offers a balanced enhancement in both transaction throughput and security for public blockchains. However, the approach requires careful management of cross-shard communication and periodic state validation to maintain consistency. Future work should focus on optimizing these aspects to further enhance the performance and security of the system. Additionally, while CBCS showed impressive throughput

gains, it was within a permissioned blockchain context, suggesting a need for context-specific optimizations in Secure Sharding for different blockchain environments.

References

- [1] X. S. Mei, W. Guo, Z. Liu, Y. M. Liu, W. J. Li, and P. Y. Zhang, "Research on blockchain scalability based on sharding strategy," in *Proc. 5th Int. Conf. Comput. Inf. Sci. Artif. Intell. (CISAI 2022)*, vol. 12566, pp. 1037–1045 (Mar. 2023), doi: 10.1117/12.2661650.
- [2] V. V. Kumar, U. Padmavathi, C. P. Ranjith, J. Balaji, and C. N. S. Vinoth Kumar, "An elixir for blockchain scalability with channel based clustered sharding," *Scalable Computing: Practice and Experience*, vol. 25, no. 2, pp. 997–1004 (2024), doi: 10.12694/scpe.v25i2.2441.
- [3] G. Viktoria and P. Borysenko, "Using sharding to improve blockchain network scalability," *System Technologies*, vol. 6, no. 143, pp. 17–27 (2022).
- [4] A. Vernekar, A. Kshirsagar, and V. K. Pachghare, "Sharding-based scalability enhancement of blockchain-based health application," in *Proc. 2023 International Conference on Circuit Power and Computing Technologies (ICCPCT)*, pp. 901–906 (Aug. 2023).
- [5] S. Tyagi and M. Kathuria, "Study on blockchain scalability solutions," in *Proc. 13th International Conference on Contemporary Computing*, pp. 394–401 (Aug. 2021).
- [6] K. Khacef, S. Benbernou, M. Ouziri, and M. Younas, "Trade-off between security and scalability in blockchain design: A dynamic sharding approach," in *Proc. International Conference on Deep Learning, Big Data and Blockchain, Cham, Switzerland: Springer International Publishing*, pp. 77–90 (Aug. 2021).
- [7] S. Toxanov, S. Sharipova, A. Biloshchytskyi, D. Abzhanova, and B. Bakytkereiuly, "Analysis of the impact of sharding on the scalability and efficiency of blockchain technologies for the creation of information-analytical systems for environmental monitoring of emissions into the environment," *Scientific Journal of Astana IT University*, no. 18, pp. 66–74 (2024), doi: 10.37943/18VIFS4010.
- [8] R. Li, Y. Qin, C. Wang, M. Li, and X. Chu, "A blockchain-enabled framework for enhancing scalability and security in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 6, pp. 7389–7400 (2022).

- [9] F. Rahman, C. Titouna, and F. Nait-Abdesselam, "Prioritised sharding: A novel approach to enhance blockchain scalability," in *Proc. 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pp. 1–2 (Oct. 2023).
- [10] A. Aldoubae, N. H. Hassan, and F. A. Rahim, "A systematic review on blockchain scalability," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 9, pp. 774–784 (2023).
- [11] F. H. N. Al-Mutar, A. A. T. Al-Khazaali, and B. A. Hataf, "Scalability of blockchain: Review of cross-sharding with high communication overhead," in *BIO Web of Conferences*, vol. 97, Art. no. 00075 (2024), doi: 10.1051/bioconf/20249700075.
- [12] V. P. Singh, S. S. Biswas, B. Alankar, and S. Tanweer, "Cryptographic modeling and discrete structures for intrusion detection in Ethereum smart contracts," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 8, pp. 3039–3048 (2025).
- [13] A. Dadhich, B. Keswani, and D. Goyal, "Comparative analysis of a novel smart contract-based hybrid access control model for blockchain-enabled secure IoT home automation systems," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 7, pp. 2875–2888 (2025).
- [14] V. Ramachandran, H. M. A. Ghanimi, B. Marapelli, N. Kaur, M. R. Laxmi, R. K. Bommisetti, S. Sengan, and P. Dadheech, "An enterprise blockchain model: A reliable cryptography-based cyber-physical systems for securing user data," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-B, pp. 2103–2114 (2025).

Received October, 2025