Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3117–3125
DOI : 10.47974/JDMSC-2696

Design and analysis of a discrete mathematical model for secure and encrypted dynamic sharding in blockchain systems

Satpal Singh Kushwaha [@]
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Sushanth Chandra Addimulam [†]
Kforce Inc.
2681 Sidney St.
Pittsburgh
PA 15203
USA

Manoj Kumar Rawat [§]
Department of Computer Science and Engineering
Medicaps University
Indore 453331
Madhya Pradesh
India

S. Sridevi [‡]
Department of Internet of Things (IoT)
Koneru Lakshmaiah Education Foundation
Guntur 522302
Andhra Pradesh
India

[@] *E-mail:* satpal.singh@jaipur.manipal.edu
[†] *E-mail:* sushanth93@gmail.com
[§] *E-mail:* manojkumar.rawat@medicaps.ac.in
[‡] *E-mail:* srisat1617@gmail.com

Ajit Noonia *
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

Blockchain sharding enhances scalability by dividing the network and ledger into parallel-processing shards, but dynamic sharding introduces security risks, especially under adaptive adversarial attacks. This paper presents a rigorous discrete mathematical framework for secure and encrypted dynamic sharding. It models shard formation, node assignment, and reconfiguration as discrete-time stochastic processes over dynamic graphs, with cryptographic hash functions ensuring secure shard allocation. Security is analyzed using combinatorics and probability theory, while a Markov-chain-based model captures system evolution under adversarial influence. The paper derives bounds on shard compromise probability using binomial distributions and Chernoff bounds. Additionally, a key-evolving encryption mechanism is introduced to ensure correct and forward-secure state transitions. Theoretical results show that shard takeover probability decreases exponentially with shard size, while encrypted state migration preserves consistency. Overall, this work provides a mathematically rigorous foundation with provable security and correctness guarantees for scalable blockchain systems.

Subject Classification: *68M25, 68N30.*

Keywords: *Discrete mathematics, Dynamic sharding, Blockchain, Secure sharding, Innovation.*

1. Introduction

Blockchain systems enable decentralized trust through replication and consensus, but this limits scalability. Sharding improves throughput by dividing the network into parallel-processing committees, though static sharding is vulnerable to adaptive attacks. Dynamic sharding mitigates this by reshuffling nodes, but introduces challenges in security, correctness, and state migration. Most existing approaches rely on algorithmic descriptions and informal or simulation-based analysis, which are insufficient for adversarial settings. Therefore, a formal discrete mathematical model [1], [2] is needed to rigorously analyze shard formation, adversarial behavior, and encrypted state transitions.

1.1 *Motivation*

As blockchain adoption grows in large-scale adversarial settings, scalable designs with formal security guarantees are needed. Sharding boosts throughput by splitting the network and ledger into smaller committees, but static shards are vulnerable to adaptive attacks, and current dynamic sharding mostly relies on

* *E-mail:* **ajit.noonia@jaipur.manipal.edu (Corresponding Author)**

heuristics and empirical results [3]. A rigorous mathematical framework capturing shard dynamics, adversaries, and secure state transitions is still missing.

1.2 *Contributions*

This paper proposes a discrete framework for secure encrypted dynamic sharding, modeling shard blockchains as discrete-time dynamic graphs with finite-field hashing, Markov-based reconfiguration, binomial/Chernoff security bounds, and key-evolving encrypted state migration to ensure consistency and forward secrecy, providing a unified basis for analyzing security, correctness, and scalability.

1.3 *Outline*

The structure of the paper is organized as follows. Section 2 reviews related work on blockchain sharding. Section 3 presents the proposed discrete mathematical framework for secure and encrypted dynamic sharding. Section 4 discusses simulation results and experimental validation that support the analytical findings. Section 5 discusses the future research challenges. Finally, Section 6 concludes the paper by summarizing the key contributions.

2. Related Work

Since the introduction of blockchain sharding, significant research has explored architectural, cryptographic, and probabilistic methods to improve scalability while maintaining security. Luu et al. [4] proposed Elastico, enabling parallel processing but relying on static shard membership, making it vulnerable to adaptive attacks. Kokoris-Kogias et al. [5] introduced OmniLedger with randomness beacons and reshuffling, though its analysis is largely empirical. Zamani, Movahedi, and Raykova [6] proposed RapidChain for high throughput using probabilistic analysis, but without modeling long-term dynamics. Buterin [7] outlined Ethereum 2.0's sharding with validator rotation under proof-of-stake, but without rigorous mathematical modeling. Pass and Shi [8] provided probabilistic guarantees for safety and liveness. Choi, Manoj, and Bonneau [9] studied secure shard assignment using random beacons and verifiable random functions, while Yu et al. [10] highlighted scalability and security challenges without a unified framework. Dang et al. [11] proposed encrypted shard state migration, though formal proofs remain limited.

3. Proposed Methodology

The proposed methodology follows a structured mathematical workflow, where each stage corresponds to a formally defined component of the dynamic sharding framework. The system is modeled using discrete-time processes, probabilistic distributions, and cryptographic mappings to ensure security and scalability.

3.1 *Blockchain Network Model*

Let the blockchain system consist of a finite set of nodes $V = \{v_1, v_2, \dots, v_N\}, | V | = N$. Each node participates in transaction validation and consensus. The network state at any time is completely characterized by the node set and their shard assignments.

3.2 *Discrete-Time Graph Representation*

Time progresses in discrete rounds $t \in \mathbb{Z}^+$. At each round, node interactions are captured using a dynamic graph $G(t) = (V, E(t)), E(t) \subseteq V \times V$.

The adjacency structure may change over time, allowing the system to be modeled as a sequence $\{G(t)\}_{t \geq 0}$. This formulation enables analysis of shard connectivity, communication overhead, and fault propagation.

3.3 *Cryptographic Shard Assignment*

At time t, the node set is partitioned into $S(t)$ disjoint shards:

$$V = \bigsqcup_{s=1}^{S(t)} V_s(t), | V_s(t) | = n_s(t) \quad (1)$$

Shard assignment is defined as a mapping $\phi_t: V \to \{1,2, \dots, S(t)\}$ Using a cryptographic hash function Hover a finite field and a public randomness beacon r_t, the assignment is computed as $\phi_t(v_i) = \big(H(v_i \parallel r_t) mod S(t)\big) + 1$

For any shard s, the expected shard size satisfies:

$$\mathbb{E}[| V_s(t) |] = \frac{N}{S(t)} \quad (2)$$

3.4 *Dynamic Shard Reconfiguration*

Let the global shard configuration at time t be denoted by $X(t) = \{V_1(t), V_2(t), \dots, V_{S(t)}(t)\}$. Shard reconfiguration is modeled as a state transition:

$$X(t+1) = f(X(t), r_{t+1}) \quad (3)$$

where r_{t+1} is independent randomness. This induces a stochastic process $\{X(t)\}_{t \geq 0}$with transition kernel $P(x, y) = \Pr[X(t+1) = y \mid X(t) = x]$

The memoryless nature of this transition allows shard evolution to be analyzed using Markov chain techniques. This step corresponds to the Dynamic Shard Reconfiguration (Markov Process). Figure 1 depicts the dynamic shard reconfiguration.

3.5 *Probabilistic Security and Encrypted State Transition Model*

Assume an adversary controls $| A | = fN$, $0 < f < 1$. For a shard of size n_s, the number of adversarial nodes $X_s \sim \text{Binomial}(n_s, f)$. A shard is compromised if $X_s \geq \alpha n_s$, $\alpha > \frac{1}{2}$, with compromise probability given in eu. 4. Each shard maintains state $\Sigma_s(t) = (L_s(t), B_s(t))$, encrypted before reconfiguration as $C_s(t) = \text{Enc}_{k_s(t)}(\Sigma_s(t))$. The key evolves as $k_s(t+1) =$

$H(k_s(t) \parallel r_{t+1})$, ensuring confidentiality and forward secrecy. Combining shard assignment, reconfiguration, adversarial modeling, and encrypted state mapping yields a secure dynamic sharding process, with global failure probability bounded as in eq. 5.

$$\Pr[X_s \geq \alpha n_s] = \sum_{k=\lceil \alpha n_s \rceil}^{n_s} \binom{n_s}{k} f^k (1-f)^{n_s-k} \tag{4}$$

$$\Pr[\exists \text{ compromised shard}] \leq S(t) \cdot \Pr[X_s \geq \alpha n_s] \tag{5}$$

4. Simulation Framework and Experimental Validation

To validate the analytical results derived in the previous sections, we conduct discrete-time simulations that model dynamic shard reconfiguration, adversarial node distribution, and shard compromise probabilities.

4.1 *Simulation Model and Parameters*

The blockchain network is simulated as a discrete-time system consistent with the formal model described in Section 3. At each simulation round, nodes are reassigned to shards using the cryptographic shard assignment function, and adversarial presence is evaluated across shards. The simulation parameters are shown in Table 1. At each round t, node-to-shard assignment is computed as $\phi_t(v_i) = (H(v_i \parallel r_t) mod S) + 1$.

Table 1

Simulation Parameters

Parameter	Symbol	Value Range
Total number of nodes	N	500 – 5000
Number of shards	S	5 – 50
Shard size	$n_s = N/S$	Derived
Adversarial fraction	f	0.10 – 0.35
Compromise threshold	α	0.50 – 0.67
Reconfiguration rounds	T	100 – 1000

4.2 *Simulation and Validation of Shard Security*

Monte Carlo simulations [12] estimate shard compromise probability under dynamic reconfiguration by randomly assigning adversarial nodes and evaluating shard compromise based on adversarial thresholds. The empirical probability is computed as:

$$\hat{P}_{\text{comp}} = \frac{1}{T \cdot S} \sum_{t=1}^{T} \sum_{s=1}^{S} \mathbf{1}[X_s(t) \geq \alpha n_s \tag{6}$$

Figure 2 (a) shows dynamic and unpredictable shard assignments across reconfiguration rounds. To validate analytical results, the empirical probability is compared with the Chernoff bound. Results closely match the theoretical exponential decay, confirming the tightness of the bound.

$$P_{\text{bound}} = \exp\left(-\frac{(\alpha - f)^2 n_s}{2f}\right) \tag{7}$$

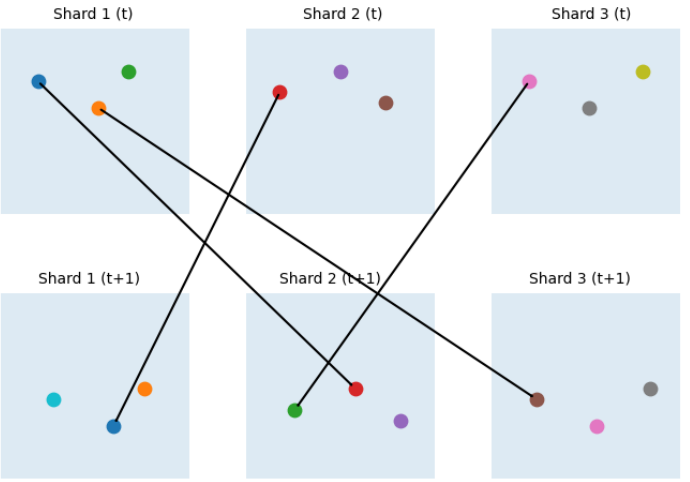

Figure 1

Dynamic Shard Reconfiguration Process

4.3 *Security, Stability, and Overhead Analysis of Dynamic Sharding*

The evaluation analyzes security, stability, and efficiency of dynamic sharding. As shown in Figure 2 (b), increasing the adversarial fraction f (with fixed shard size) sharply increases compromise probability as f approaches α, highlighting the condition $f < \alpha$. Markovian stability [13] is validated through $Pr(X(t+1)=x \mid X(t)=y)$, with the Figure 3 heatmap confirming memoryless, time-homogeneous behavior. Encrypted state migration overhead is evaluated via T_enc and T_dec against $|\Sigma_s|$, showing linear complexity ($T_{enc}, T_{dec} \in O(|\Sigma_s|)$) as in Figure 2 (c). Overall, results confirm exponential decay in compromise probability with shard size, effective adversarial mitigation via reconfiguration, and secure migration with acceptable overhead, with minor deviations due to finite sampling.

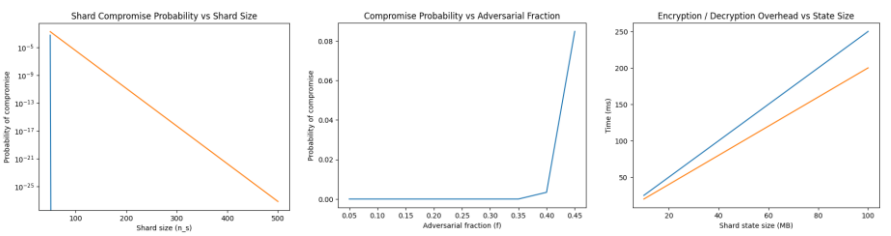

Figure 2

(a) Shard Compromise Probability vs. Shard Size, (b) Compromise Probability vs. Adversarial Fraction, (c) Encryption Overhead vs. Shard State Size

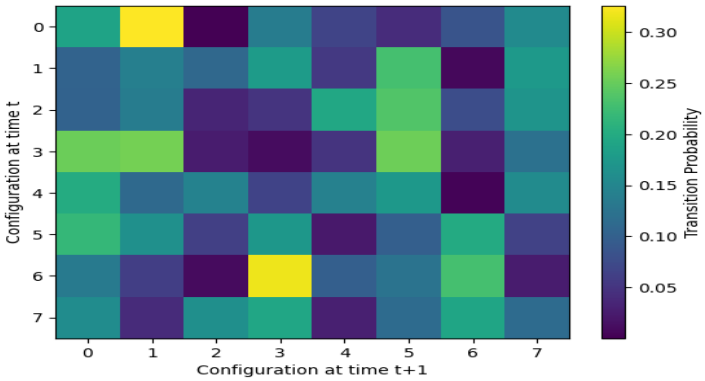

Figure 3

Transition Probability Heatmap

5. Limitations and Future Research Directions

Despite its strong theoretical guarantees, the framework has limitations. It assumes a fixed, uniformly distributed adversary and does not account for stake-weighted or heterogeneous settings, while simulations abstract network factors like latency and cross-shard overhead. Future work will extend the model to adaptive and stake-weighted adversaries, incorporate network and cross-shard dynamics, and apply game-theoretic analysis to study incentives, strategic behavior, and long-term stability.

6. Conclusion

This paper presents a discrete mathematical framework for secure, encrypted dynamic sharding in blockchain systems. Shard-based blockchains are modeled as discrete-time dynamic graphs with stochastic reconfiguration, enabling formal security analysis. The framework uses cryptographically secure hash-based shard assignment, derives exponential bounds on shard compromise, and incorporates key-evolving encrypted state transitions to ensure confidentiality and forward secrecy. Simulation results validate the theoretical analysis and demonstrate the practicality of encrypted shard migration, providing a unified foundation for secure and scalable dynamic sharding.

References

[1] 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).

[2] 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).

[3] 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).

[4] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, pp. 17–30 (Oct. 2016).

[5] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," in *Proc. IEEE Symp. Security Privacy (SP*), pp. 583–598 (May 2018).

[6] M. Zamani, M. Movahedi, and M. Raykova, "Rapidchain: Scaling blockchain via full sharding," in *Proc. 2018 ACM SIGSAC Conf. Comput. Commun. Security (CCS),* pp. 931–948 (Oct. 2018).

[7] V. Buterin, "Sharding FAQ," Vitalik Buterin's Website, (Dec. 31, 2017). [Online]. Available: https://vitalik.eth.limo/general/2017/12/31/sharding_faq.html. [Accessed: Jul. 17, 2025].

[8] R. Pass and E. Shi, "The sleepy model of consensus," in *Proc. Int. Conf. Theory Appl. Cryptology Inf. Security (ASIACRYPT)*, pp. 380–409 (Nov. 2017).

[9] K. Choi, A. Manoj, and J. Bonneau, "SoK: Distributed randomness beacons," in *Proc. IEEE Symp. Security Privacy (SP),* pp. 75–92 (May 2023).

[10] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu, "Survey: Sharding in blockchains," *IEEE Access,* vol. 8, pp. 14155–14181 (2020).

[11] H. Dang, T. T. A. Dinh, D. Loghin, E. C. Chang, Q. Lin, and B. C. Ooi, "Towards scaling blockchain systems via sharding," in *Proc. 2019 Int. Conf. Management Data (SIGMOD)*, pp. 123–140 (June 2019).

[12] S. Raychaudhuri, "Introduction to Monte Carlo simulation," in *Proc. Winter Simulation Conf. (WSC)*, pp. 91–100 (Dec. 2008).

[13] S. P. Meyn and R. L. Tweedie, "Stability of Markovian processes I: Criteria for discrete-time chains," *Adv. Appl. Probab.*, vol. 24, no. 3, pp. 542–574 (1992).

Received December, 2025