

**A security aware discrete mathematics framework for
Nash-equilibrium based incentive design against selfish mining and
validator collusion**

Satpal Singh Kushwaha[@]

Department of Computer Science and Engineering

Manipal University Jaipur

Jaipur 303007

Rajasthan

India

Pradeep Gupta⁺

Department of Computer Science and Engineering

Ajay Kumar Garg Engineering College

Ghaziabad 201015

Uttar Pradesh

India

Lipika Goel[§]

Department of Computer Science and Engineering (AIML)

Sridevi Women's Engineering College

Hyderabad 500075

Telangana

India

Y. Lakshmi Prasanna[‡]

Department of Computer Science and Information Technology

Koneru Lakshmaiah Education Foundation

Hyderabad 500043

Telangana

India

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

⁺ E-mail: gupta.pradeep85@gmail.com

[§] E-mail: lipika.bose@gmail.com

[‡] E-mail: prasanna.yeluri@gmail.com

Sonam Gupta *

*Department of Computer Science and Engineering
Ajay Kumar Garg Engineering College
Ghaziabad 201015
Uttar Pradesh
India*

Abstract

Blockchain networks depend on incentive mechanisms to ensure that rational miners/validators follow the prescribed consensus protocol. However, strategic behavior such as selfish mining, validator collusion, and reward manipulation can degrade security, decentralization, and fairness. This paper proposes a game-theoretic framework to model and analyze incentive compatibility in blockchain systems. We formalize the interaction among participants as non-cooperative and coalition games, where agents choose between honest participation, selfish deviation, or collusive coordination. A mathematical payoff model is developed incorporating reward distribution, operational costs, detection probabilities, and penalty/slashing functions. Nash equilibrium conditions are derived to characterize when honest participation becomes a stable equilibrium. We further introduce a fairness-aware reward shaping mechanism that reduces the profitability of selfish strategies while discouraging collusion through coalition-dependent penalties. The framework provides explicit equilibrium constraints and design insights for secure and fair incentive mechanisms in both Proof-of-Work and Proof-of-Stake blockchain networks.

Subject Classification: 68M25, 68N30.

Keywords: Blockchain incentives, Game theory, Nash equilibrium, Selfish mining, Validator collusion.

1. Introduction

Blockchain consensus protocols allow decentralized agreement among untrusted participants without a central authority, ensuring a consistent ledger despite delays, partial information, and adversarial conditions [1]. While cryptography and distributed systems provide integrity and fault tolerance, they are insufficient alone in open, permissionless settings. Thus, blockchains require incentive mechanisms that align participants' self-interest with correct protocol behavior [2]. Since miners/validators are rational and driven by rewards, costs, and risks, they may adopt strategies like selfish mining or block withholding if profitable, potentially undermining fairness, decentralization, and security [3].

1.1 Motivation

Blockchain incentives are often more vulnerable to rational manipulation than to direct cryptographic attacks, as economically motivated miners/validators may deviate whenever it increases expected profit. This enables threats such as selfish mining, validator collusion, and reward unfairness, which can reduce trust, weaken decentralization, and threaten long-

* E-mail: guptasonam6@gmail.com (Corresponding Author)

term network security. Therefore, incentive mechanisms must be designed to be both functional and game-theoretically robust against strategic behavior.

1.2 Contributions

This paper presents a security-aware, game-theoretic framework for blockchain incentive design, modeling miners/validators as utility-maximizing agents. It defines a payoff model and derives Nash equilibrium conditions to ensure honest participation, extends to collusion via coalition-game constraints, and incorporates fairness-aware reward shaping to support decentralization without breaking incentives. Overall, it provides explicit conditions to reduce selfish mining and validator collusion.

1.3 Outline

The paper is organized as follows. Section 2 reviews related work on selfish mining, validator collusion, and incentive fairness in blockchain networks. Section 3 presents the proposed security-aware discrete mathematics framework for Nash-equilibrium based incentive design. Section 4 discusses simulation results and validation. Section 5 highlights limitations and future work. Finally, Section 6 concludes the paper.

2. Related Work

Nakamoto [4] Bitcoin protocol assumes that honest participation dominates when a majority of computational power follows the protocol. Eyal and Sirer [5] showed that selfish mining can outperform honest mining under certain hash power and network conditions, proving that correctness does not guarantee incentive compatibility. Sapirshtein, Sompolinsky, and Zohar [6] optimized selfish mining using a Markov decision process, demonstrating higher profitability under refined strategies. Nayak et al. [7] extended this to stubborn mining and highlighted how network delays and connectivity strengthen withholding-based deviations. Karame et al. [8] analyzed double-spending and confirmation security under probabilistic assumptions. Sompolinsky and Zohar [9] emphasized that latency and fork rates significantly influence both security and incentive outcomes. Ouroboros [10] provided formal security foundations for Proof-of-Stake consensus.

3. Proposed Methodology

This section presents the formal framework, including the system model, payoff construction, equilibrium analysis, collusion modeling, and fairness-aware reward design.

3.1 Framework Overview and System Model

This work proposes a security-aware discrete mathematics framework for Nash-equilibrium [11], [12] based incentive design in blockchain networks. The framework jointly models honest vs selfish behavior, validator collusion through coalition formation, and reward fairness through shaping. Consider n participants

$\mathcal{N} = \{1, 2, \dots, n\}$, where agent i controls resource $x_i \geq 0$. The total resource X and normalized influence α_i are defined in (1), ensuring proportional representation of hash power or stake. The per-block reward and operational cost are modeled in (2), and each agent selects an action from the discrete strategy set $\mathcal{A}_i = \{H, S, C\}$ as stated in (2).

$$X = \sum_{i=1}^n x_i, \alpha_i = \frac{x_i}{X} \quad (1)$$

$$B = R + F, c_i(x_i) = kx_i^\gamma, \mathcal{A}_i = \{H, S, C\} \quad (2)$$

3.2 Payoff Model and Nash-Equilibrium Formulation

Participants are modeled as rational utility-maximizing agents. The expected utility of agent i under strategy profile $\mathbf{a}$ is defined in (3), combining expected rewards, operational costs, and penalty/slashing terms. Under full honesty, proportional allocation yields the baseline utility in (4), which is used as the reference point for deviation analysis. The strategic interaction forms a finite game, and Nash equilibrium is enforced using the unilateral deviation constraint in (5), which is the core stability condition required for incentive-compatible consensus.

$$u_i(\mathbf{a}) = \mathbb{E}[r_i(\mathbf{a})] - c_i(x_i) - \pi_i(\mathbf{a}) \quad (4)$$

$$u_i(H) = \alpha_i B - c_i(x_i) \quad (5)$$

$$u_i(a_i^*, \mathbf{a}_{-i}^*) \geq u_i(a_i, \mathbf{a}_{-i}^*), \forall i \quad (6)$$

3.3 Selfish Mining Deterrence Condition

Selfish mining is modeled using a deviation gain function $\Delta(\alpha_i) \geq 0$, which increases the effective reward share of agent i . The selfish payoff function is expressed in (6), where $p_i \geq 0$ denotes the expected penalty imposed on selfish behavior. Using the honest baseline utility from (4) and comparing it with the selfish payoff in (6), the Nash-equilibrium deterrence constraint in (7) is derived, ensuring that selfish deviation is not profitable.

$$u_i(S) = (\alpha_i + \Delta(\alpha_i))B - c_i(x_i) - p_i \quad (6)$$

$$u_i(H) \geq u_i(S) \Rightarrow p_i \geq B\Delta(\alpha_i) \quad (7)$$

3.4 Collusion Resistance via Coalition-Proof Constraints

To capture validator collusion, we consider any coalition $S \subseteq \mathcal{N}$. The collusion gain is modeled in (8) as a function of coalition influence α_S , where parameters λ and β represent the strength and growth rate of coalition advantage. To discourage cartel formation, coalition-level penalties $P(S)$ must dominate the collusion gain, which is enforced through the coalition-proof stability condition in (9).

$$G(\alpha_S) = \lambda \alpha_S^\beta B \quad (8)$$

$$P(S) \geq G(\alpha_S) = \lambda \alpha_S^\beta B \quad (9)$$

3.5 Security-Aware Reward Shaping for Decentralization Preservation

Reward fairness is incorporated to reduce long-term concentration risk and support decentralization. Fairness deviation and distribution equality are quantified using the loss function $\Phi(r)$ and Jain's fairness index $J(r)$, both defined in (10). Based on these fairness metrics, the proposed shaping rule in (11) adjusts rewards using measurable honest behavior signals h_i and deviation indicators g_i , where θ and μ control fairness reinforcement and deterrence strength.

$$\Phi(r) = \sum_{i=1}^n (r_i - r_i^*)^2, J(r) = \frac{(\sum_i r_i)^2}{n \sum_i r_i^2} \quad (10)$$

$$r_i = \alpha_i B + \theta h_i - \mu g_i \quad (11)$$

3.6 Integrated Nash and Coalition-Proof Security Conditions

The framework jointly enforces incentive security by combining individual deviation deterrence in (7) and coalition-proof stability in (9), while improving fairness through the shaping rule in (11). To quantify system-level efficiency, social welfare is defined in (12) as the sum of participant utilities, where utilities follow the payoff structure of (3). The Price of Anarchy in (13) measures the efficiency gap between Nash outcomes and the socially optimal welfare, and improving incentive compatibility through (7) and (9) increases the likelihood of high-welfare equilibrium outcomes.

$$W(a) = \sum_{i=1}^n u_i(a) \quad (12)$$

$$PoA = \frac{W^{NE}}{W^*}, 0 < PoA \leq 1 \quad (13)$$

4. Simulation Framework and Experimental Validation

This section validates the proposed security-aware discrete mathematics framework for Nash-equilibrium based incentive design in blockchain networks under rational and coalition-based adversaries.

4.1 Selfish Mining Deterrence via Nash-Equilibrium Penalty

Selfish mining is evaluated by comparing honest payoff $u(H) = \alpha B - c(x)$ with selfish payoff $u(S) = (\alpha + \Delta(\alpha))B - c(x) - p$, giving the deviation advantage. Eq. (16) shows that selfish mining is profitable if and only if $p < B\Delta(\alpha)$. The break-even point occurs at p^* . For $p \geq p^*$, the advantage becomes non-positive, making honest mining the stable best response. Thus, Nash-equilibrium penalties can eliminate selfish mining profitability. The honest-stability region defines the penalty levels that ensure honest behavior across miner influence α .

$$u(S) - u(H) = B\Delta(\alpha) - p. \quad (16)$$

$$p^* = B\Delta(\alpha), \quad (17)$$

$$\mathcal{R}_H = \{(\alpha, p) \mid p \geq B\Delta(\alpha)\}. \quad (18)$$

4.2 Collusion Incentives and Coalition Growth

Validator collusion is modeled using coalition influence α_S , where the gain is:

$$G(\alpha_S) = \lambda \alpha_S^\beta B, \lambda \geq 0, \beta \geq 1. \quad (19)$$

For $\beta > 1$, gains grow superlinearly, meaning larger coalitions gain disproportionately, creating centralization pressure. To ensure stability, penalties must outweigh gains:

$$P(S) \geq G(\alpha_S) = \lambda \alpha_S^\beta B. \quad (20)$$

This implies penalties must scale with coalition influence to deter collusion. The coalition-stability region is defined as

$$\mathcal{R}_C = \{(\alpha_S, P) \mid P \geq \lambda \alpha_S^\beta B\}. \quad (21)$$

Figure 2 (b) shows that for larger α_S , the required penalty P grows rapidly, which supports the conclusion that coalition-aware penalties are essential for decentralization preservation.

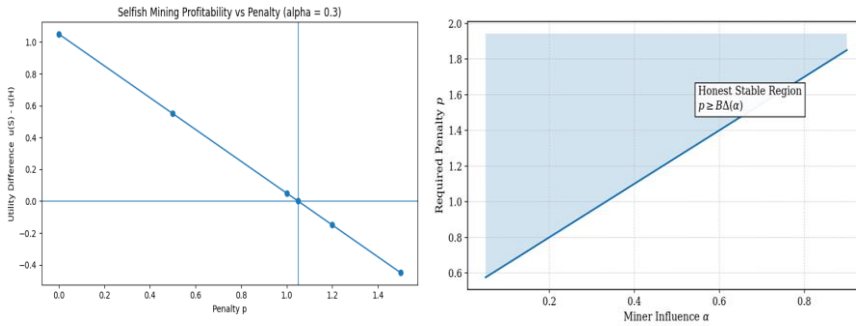


Figure 1

(a) Selfish mining profitability vs. penalty p , (b) Nash stability region $\mathcal{R}_H$ showing the boundary $p=BA(\alpha)$ for honest participation

4.3 Comparative Security Effectiveness Under Joint Threats

To evaluate combined security strength, we define a unified “incentive-security margin” capturing both individual and coalition resistance:

$$\mathcal{M} = \min(p - B\Delta(\alpha), P(S) - \lambda \alpha_S^\beta B). \quad (22)$$

When $\mathcal{M} \geq 0$, selfish mining and collusion are deterred under Nash and coalition-proof constraints; $\mathcal{M} < 0$ means at least one deviation is still profitable. Thus, $\mathcal{M}$ is a compact security metric for comparing parameters. Figure 2 (c) shows higher penalties reduce selfish mining linearly (Eq. 17) but collusion deterrence grows nonlinearly (Eq. 19), requiring stronger scaling for coalition security. Overall, Figure 1 (a) and 1 (b) (Eq. 16–18) confirm equilibrium

penalties remove selfish mining profits, while Figure 2 (a) and Figure 2 (b) (Eq. 19–21) show collusion gains rise quickly with coalition size, demanding coalition-aware penalties. Eq. (22) and Figure 2 (c) validate the framework as a mathematically grounded approach for incentive-compatible consensus against rational and coalition adversaries.

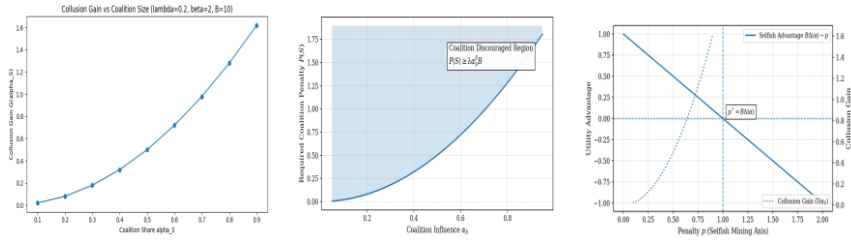


Figure 2

(a) Collusion gain $G(\alpha_S)$ as a function of coalition size α_S , (b) Coalition-proof deterrence region R_C , (c) Selfish deviation suppression vs coalition deterrence growth

5. Limitations and Future Research Directions

This study has limitations that suggest future improvements to the proposed framework. The selfish mining gain $\Delta(\alpha)$ can be refined with detailed network dynamics, and the collusion benefit $G(\alpha_S)$ needs empirical validation due to MEV and censorship effects. The fairness mechanism relies on reliable honesty signals, which are difficult to make manipulation-resistant. Future work will explore mixed and repeated games, include reputation effects, model stochastic block arrivals, study dynamic coalitions, and validate results using real PoW and PoS simulations.

6. Conclusion

This work presented a security-aware discrete mathematics framework for Nash-equilibrium based incentive design in blockchain networks, addressing selfish mining, validator collusion, and reward fairness. Using payoff-based modeling and equilibrium constraints, we derived explicit penalty conditions that enforce honest participation as a Nash equilibrium and ensure coalition-proof stability against collusion. A fairness-aware reward shaping mechanism was also introduced to reduce reward concentration and support decentralization. The results demonstrate that appropriately designed penalties and fairness adjustments can jointly strengthen security and fairness in blockchain consensus environments.

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," *J. Discrete Math. Sci. Cryptogr.*, 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," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 7, pp. 2875–2888 (2025).
- [3] V. Ramachandran, H. M. A. Ghanimi, B. Marapelli, N. Kaur, M. R. Laxmi, R. K. Bommiseti, S. Sengan, and P. Dadheech, "An enterprise blockchain model: A reliable cryptography-based cyber-physical systems for securing user data," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 5-B, pp. 2103–2114 (2025).
- [4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *White Paper* (2008). [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [5] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102 (Jul. 2018).
- [6] A. Sapirshstein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in Bitcoin," in *Proc. Int. Conf. Financial Cryptography and Data Security (FC)*, Berlin, Germany, pp. 515–532 (Feb. 2016).
- [7] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in *Proc. IEEE Eur. Symp. Security Privacy (EuroS&P)*, Saarbrücken, Germany, pp. 305–320 (Mar. 2016).
- [8] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, "Misbehavior in Bitcoin: A study of double-spending and accountability," *ACM Trans. Inf. Syst. Secur.*, vol. 18, no. 1, pp. 1–32 (2015).
- [9] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in Bitcoin," in *Proc. Int. Conf. Financial Cryptography and Data Security (FC)*, Berlin, Germany, pp. 507–527 (Jan. 2015).
- [10] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proc. Annu. Int. Cryptology Conf. (CRYPTO)*, Cham, Switzerland, pp. 357–388 (Jul. 2017).

- [11] S. Mssassi and A. Abou El Kalam, "Game theory-based incentive design for mitigating malicious behavior in blockchain networks," *J. Sensor Actuator Netw.*, vol. 13, no. 1, Art. no. 7 (2024).
- [12] W. Tang, E. Liu, W. Ni, X. Qu, B. Huang, K. Li, D. Niyato, and A. Jamalipour "Game-theoretic incentive mechanism for blockchain-based federated learning," *IEEE Trans. Mobile Comput.*, early access (2025), doi: 10.1109/TMC.2025.3567355.s

Received January, 2026