EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2025, Vol. 18, Issue 4, Article Number 6555
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

A Multi-Level Optimization Framework for Blockchain Security: Integrating Metaheuristics, Reinforcement Learning, and Game Theory

Kassem Danach[1,*], Abbas Tarhini[2], Wael Hosny Fouad Aly[3], Hussin Jose Hejase[1]

[1] *Basic and Applied Sciences Research Center, Al Maaref University, Beirut, Lebanon*
[2] *Department of Computer Science, Lebanese American University, Beirut, Lebanon*
[3] *College of Engineering and Technology, American University of the Middle East, Kuwait*

Abstract. Blockchain technology relies on cryptographic mechanisms for transaction security and data integrity. However, the growing computational complexity, high transaction costs, and scalability issues pose significant challenges to blockchain adoption. Traditional cryptographic methods—such as hashing, key generation, encryption, and decryption—introduce excessive computational overhead, leading to energy inefficiencies and increased latency. This research proposes an optimization-driven crypto analysis framework that integrates metaheuristic algorithms, combinatorial optimization, reinforcement learning, and game theory to enhance the efficiency and security of blockchain cryptographic processes. The framework focuses on optimized cryptographic computation, gas fee reduction in smart contracts, security enhancement against cryptanalysis, and improved scalability of consensus mechanisms. Experimental evaluations demonstrate up to 39.4% reduction in cryptographic execution time, 29.4% savings in smart contract gas fees, and 33.3% improvement in decentralization of Proof-of-Stake validators. These results validate the effectiveness of the proposed framework in achieving secure, scalable, and cost-efficient blockchain operations.

2020 Mathematics Subject Classifications: 68M14, 68T20, 90C59

Key Words and Phrases: cryptography, blockchain security, optimization, metaheuristics, reinforcement learning, game theory

1. Introduction

Blockchain technology has revolutionized digital transactions by enabling secure, decentralized, and tamper-resistant data management [1, 2]. Cryptographic mechanisms, including hash functions, asymmetric encryption, digital signatures, and zero-knowledge

[*] Corresponding author.

DOI: https://doi.org/10.29020/nybg.ejpam.v18i4.6555

Email addresses: kassem.danach@mu.edu.lb (K. Danach), wael.aly@aum.edu.kw (W. H. F. Aly)

proofs (ZKPs), form the backbone of blockchain security [3, 4]. These methods ensure transaction integrity, identity authentication, and resistance against malicious attacks [5].

Despite these advantages, blockchain suffers from notable limitations. Computational inefficiency, especially in cryptographic operations such as SHA-256 hashing in Bitcoin, hampers scalability and increases energy usage [6]. Smart contracts on Ethereum, for instance, incur high gas fees due to suboptimal cryptographic execution, limiting the practical scalability of decentralized applications (DApps) [7]. Additionally, the rise of quantum computing and (artficial intelligence) AI-driven cryptanalysis introduces new threats to traditional cryptographic schemes [8].

Recent studies, [9, 10], have investigated metaheuristic optimization and AI-enhanced cryptographic strategies to address these inefficiencies. However, most of these solutions treat optimization as an isolated layer, failing to unify cryptographic efficiency, security robustness, and computational cost under a comprehensive framework.

Reinforcement learning (RL), known for its effectiveness in complex decision-making, has shown promise in blockchain applications [11, 12]. Unlike static heuristics, RL enables systems to adapt dynamically through real-time feedback, allowing continuous optimization of cryptographic parameters, gas fees, and consensus strategies. Advanced RL models such as Deep Q-Networks (DQN) and Proximal Policy Optimization (PPO) have been employed to fine-tune elliptic curve cryptography (ECC) parameters and smart contract logic [13]. Moreover, multi-agent RL approaches have enhanced load balancing and energy efficiency in Proof of Work (PoW) and Proof of Stake (PoS) systems [14].

Nevertheless, challenges remain. Many RL models lack explainability, struggle with convergence in cryptographic contexts, and are difficult to align with evolving threat models. These gaps motivate the current research, which proposes a multi-level optimization framework that integrates metaheuristics, reinforcement learning, and game-theoretic reasoning to holistically improve blockchain security and efficiency.

This paper addresses key challenges in blockchain systems, including computational inefficiency in cryptographic operations, high smart contract gas fees, security threats from emerging technologies, and suboptimal consensus mechanism performance [2, 15]. The proposed framework introduces four core innovations: (1) metaheuristic optimization (e.g., Genetic Algorithms, Simulated Annealing, Particle Swarm Optimization) for enhancing cryptographic performance; (2) multi-objective optimization for reducing smart contract gas fees in Ethereum and Hyperledger systems; (3) reinforcement learning-based detection of cryptographic vulnerabilities; and (4) game-theoretic models (e.g., Nash Equilibrium, Stackelberg games) for optimizing validator strategies in consensus mechanisms.

The structure of the paper is as follows. Section 2 provides a comprehensive review of existing work in cryptographic optimization and blockchain security. Section 3 introduces the proposed multi-level optimization framework in detail. Section 4 describes the experimental setup and presents the performance evaluation results. Section 5 analyzes the improvements in performance and efficiency achieved through the multi-level optimization approach. Finally, Section 6 summarizes the key findings and suggests avenues for future research.

2. Related Work

Blockchain security is fundamentally built on cryptographic primitives, yet the increasing complexity of blockchain networks demands efficient cryptographic optimization. Recent research has explored the application of metaheuristics, AI-driven cryptanalysis, and game-theoretic optimizations to enhance blockchain security and efficiency. This section reviews existing approaches in cryptographic optimization for blockchain security, smart contract efficiency, and consensus mechanisms.

2.1. Cryptographic Optimization in Blockchain Security

Cryptographic techniques such as hash functions, asymmetric encryption, and zero-knowledge proofs (ZKPs) are fundamental to ensuring the security and integrity of blockchain transactions [3, 4]. These mechanisms safeguard data authenticity, prevent double-spending, and enable privacy-preserving transactions in decentralized environments. However, traditional cryptographic methods are computationally intensive, leading to high latency, resource consumption, and scalability issues, particularly in high-throughput blockchain networks such as Ethereum and Hyperledger [8]. Additionally, the rise of AI-driven cryptanalysis and quantum computing threats has raised concerns about the long-term viability of existing cryptographic protocols [16, 17].

To address these challenges, researchers have explored metaheuristic optimization techniques to enhance cryptographic efficiency while maintaining security guarantees. For instance, Das et al. [9] applied Genetic Algorithms (GA) and Simulated Annealing (SA) to optimize hash function performance, resulting in a 30% reduction in computational overhead while preserving cryptographic strength. Similarly, Mukherjee et al. [10] proposed an adaptive cryptographic tuning mechanism using Deep Q-Networks (DQN), which dynamically adjusts cryptographic parameters such as key size, iteration count, and entropy levels, improving security without excessive computational costs. Their findings demonstrate that reinforcement learning (RL) models can effectively balance security robustness and performance efficiency.

Beyond hash function optimization, quantum-safe cryptographic protocols have also been explored. Dai et al. [18] investigated lattice-based encryption schemes optimized using Swarm Intelligence (SI) techniques, achieving significant improvements in encryption speed and post-quantum security. Another study by Wang et al. [19] introduced a hybrid cryptographic framework combining Elliptic Curve Cryptography (ECC) with Reinforcement Learning, which enhances transaction security while reducing encryption overhead by up to 25%.

Despite these advancements, most existing studies focus on isolated cryptographic functions rather than developing an integrated framework that simultaneously optimizes multiple security layers, including hashing, encryption, and privacy-preserving mechanisms. Additionally, the interaction between cryptographic optimization and blockchain scalability remains an underexplored area. Future research should investigate hybrid metaheuristic-AI optimization frameworks that integrate evolutionary algorithms, reinforcement learning, and quantum-resistant cryptographic techniques to enhance blockchain security while ensuring computational feasibility.

This research proposes a multi-layer cryptographic optimization framework that leverages metaheuristic search algorithms, reinforcement learning, and game-theoretic security models to dynamically adjust cryptographic parameters based on blockchain network conditions. The proposed approach seeks to reduce gas fees, improve transaction efficiency, and enhance resistance to AI-driven and quantum-enabled cryptographic attacks.

2.2. Smart Contract Optimization

Smart contracts enable automated transactions on blockchain platforms such as Ethereum and Hyperledger, facilitating trustless execution of decentralized applications (DApps). However, their execution is often computationally expensive due to inefficient cryptographic operations, redundant computation, and high gas fees, which hinder large-scale adoption [2, 20]. The cost of executing smart contracts is primarily influenced by the underlying virtual machine execution, storage operations, and cryptographic verifications, leading to performance bottlenecks and increased transaction fees [7].

To mitigate these inefficiencies, researchers have explored multi-objective optimization techniques and resource allocation strategies. For instance, Androulaki et al. [7] proposed an optimized cryptographic execution model in Hyperledger Fabric, demonstrating a 25% reduction in computational overhead and gas fees by leveraging improved storage handling and optimized cryptographic signatures. Similarly, Dai et al. [21] investigated transaction batching strategies and adaptive gas limit adjustments to minimize blockchain transaction costs while maintaining security guarantees. Their study revealed that a dynamic gas pricing strategy based on predictive models could reduce execution costs by up to 30% compared to static gas pricing mechanisms.

Recent advancements in AI-driven contract optimization have further improved smart contract efficiency. Reinforcement learning (RL)-based models have been employed to dynamically adjust gas fees and execution priorities, enhancing throughput and cost-effectiveness [8]. Specifically, Wang et al. [22] applied Deep Q-Learning to Ethereum smart contracts, achieving an 18% reduction in average execution costs by intelligently selecting optimal execution pathways. Additionally, actor-critic RL models have been integrated into smart contract execution engines to optimize transaction bundling, significantly reducing network congestion [23].

Despite these advances, most existing studies focus on isolated optimizations and do not holistically integrate metaheuristic optimization with cryptographic efficiency improvements. Hybrid approaches that combine genetic algorithms (GA), simulated annealing (SA), and swarm intelligence techniques with reinforcement learning could further enhance the adaptability and efficiency of smart contracts [24]. Furthermore, game-theoretic models have been proposed to optimize miner incentives for cost-effectively executing smart contract, yet they remain underexplored in real-world implementations [25].

This research aims to bridge these gaps by proposing a hybrid optimization framework that integrates metaheuristics, reinforcement learning, and cryptographic enhancements to optimize smart contract execution. By leveraging adaptive gas pricing, transaction prioritization, and cryptographic cost minimization, the proposed framework seeks to achieve efficient, scalable, and cost-effective smart contract execution in blockchain environments.

2.3. Blockchain Consensus Mechanisms and Optimization

Consensus mechanisms, including Proof-of-Work (PoW) and Proof-of-Stake (PoS), are foundational components in blockchain networks, responsible for maintaining security, achieving distributed agreement, and validating transactions [1, 15]. PoW mechanisms, as employed by Bitcoin, rely on computationally intensive puzzles that ensure security through substantial energy expenditure. While effective, this approach has been widely criticized for its unsustainable energy consumption and environmental impact, limiting scalability and practical deployment in resource-constrained settings.

In contrast, PoS consensus protocols select validators based on the amount of cryptocurrency they stake, significantly reducing energy usage compared to PoW. However, PoS systems introduce their own challenges, primarily related to the fairness and efficiency of validator selection processes. One major concern is stake centralization, where large stakeholders can disproportionately influence consensus outcomes, potentially undermining the decentralization and trustworthiness of the network [6].

To mitigate these issues, researchers have increasingly turned to game-theoretic modeling and optimization techniques. Game theory provides a rigorous framework to analyze strategic interactions among validators, enabling the design of incentive mechanisms that promote fair stake distribution and robust network participation. For instance, Bano et al. [6] applied Nash equilibrium and Stackelberg game models to optimize validator selection, demonstrating how these approaches can effectively reduce centralization risks while preserving consensus security. Their work highlights the importance of equilibrium-based strategies to balance validator rewards and operational costs.

Further advancements have explored the integration of metaheuristic optimization algorithms to enhance PoS performance metrics. Hassanzadeh-Nazarabadi et al. [8] investigated the use of metaheuristics for tuning mining reward schemes, resulting in a significant 18% increase in transaction throughput. This approach exemplifies how adaptive optimization techniques can dynamically adjust system parameters to improve scalability and responsiveness without compromising security.

These studies underscore the potential of combining game theory and metaheuristic optimization to address critical limitations in PoS consensus protocols, paving the way for more efficient, fair, and sustainable blockchain architectures.

2.4. Research Gaps and Proposed Framework

Although significant progress has been made in blockchain cryptographic optimization, several critical gaps persist in the literature. First, there is a lack of an integrated optimization framework that jointly considers cryptographic efficiency, consensus mechanism performance, and transaction cost reduction. Most existing studies [26–29] tend to focus on individual components in isolation—such as improving encryption speed or refining validator selection—without adopting a unified strategy that balances security, efficiency, and scalability.

Second, the application of machine learning, particularly reinforcement learning, in real-time cryptanalysis and dynamic security adaptation remains underexplored. While AI techniques have been successfully applied to parameter tuning and heuristic selection, their full potential in adaptive threat detection and mitigation within blockchain environments is yet to be realized. Third, although game theory has been widely used for theoretical modeling of Proof-of-Stake (PoS) consensus, practical implementations of these models in real-world blockchain systems like Ethereum 2.0 or Tezos are still lacking [30]. This limits the effectiveness of validator incentive schemes and resource allocation strategies.

To address these limitations, this research proposes an Optimization-Driven Crypto Analysis Framework that integrates metaheuristic algorithms, reinforcement learning, and game-theoretic modeling. The framework introduces three core innovations: (1) metaheuristic and AI-based cryptographic optimization to reduce computational overhead and improve transaction throughput; (2) multi-objective optimization for smart contract execution, aimed at minimizing gas fees without compromising security; and (3) game-theoretic consensus optimization, improving validator selection, stake distribution, and overall network resilience. By bridging these complementary approaches, the proposed framework aims to deliver a secure, efficient, and scalable blockchain architecture capable of withstanding evolving cryptographic threats.

Recent studies have explored a wide range of optimization and intelligence-driven techniques to improve network performance, cryptographic efficiency, and system resilience in emerging computing paradigms. Aly et al. [31, 32] examined SDN controller placement and architecture using dynamic feedback and machine learning models to reduce latency and improve adaptability, which aligns with our focus on cryptographic optimization within complex, distributed networks. Similarly, multi-agent and agent-based modeling approaches have been employed for risk analysis and system planning in uncertain environments [33, 34], offering valuable insights into designing decentralized and resilient frameworks akin to those used in blockchain. Studies on trust-aware task offloading and fairness in edge-fog-cloud systems [35] further reinforce the utility of multi-criteria decision-making (MCDM) frameworks, an idea echoed in our game-theoretic optimization layer. Other works have addressed secure and low-complexity communication schemes [36], UAV service location planning during crises [37], and fake news detection through embedding-based learning models [38], all of which underline the broader applicability of AI and optimization in enhancing the security, efficiency, and intelligence of distributed digital systems. In addition, investigations into specialized modeling techniques, such as Hidden Markov Models [39] and spectral element methods [40], demonstrate the growing emphasis on adaptive computational frameworks for robust analysis—core to the reinforcement learning and optimization techniques employed in our proposed system.

3. Methodology of the Optimization-Driven Crypto Analysis Framework for Blockchain Security and Efficiency

This section presents the proposed **Optimization-Driven Crypto Analysis Framework**, designed to enhance blockchain security and efficiency through the integration of *metaheuristic optimization, reinforcement learning-based cryptanalysis, and game-theoretic consensus modeling.* The methodology is organized into six key components: problem formulation, proposed framework, optimization techniques, implementation strategy, mathematical formulation, and expected outcomes.

3.1. Problem Formulation

Blockchain systems rely heavily on cryptographic computations, smart contract execution, and consensus mechanisms to ensure security, trust, and efficiency. However, the increasing complexity of these components introduces significant computational overhead, energy consumption, and scalability limitations. The central objective of this research is to **minimize computational cost** while **maximizing security and scalability** by optimizing the following three aspects:

- **Cryptographic Computation:** Reduce the execution time of encryption, hashing, and signature verification while preserving cryptographic strength.
- **Smart Contract Optimization:** Minimize gas fees and latency in Ethereum-based smart contracts using multi-objective learning.
- **Consensus Mechanism Efficiency:** Improve Proof-of-Stake (PoS) validator selection and reward fairness using game-theoretic equilibrium models.

This problem is formalized as a constrained multi-objective optimization task:

$$\min_{x} \quad C(x) = \alpha \cdot T(x) + \beta \cdot E(x) + \gamma \cdot S(x) \tag{1}$$

$$\text{Subject to: } T(x) \leq T_{\max}, \quad E(x) \leq E_{\max}, \quad S(x) \geq S_{\min} \tag{2}$$

where

- $T(x)$: Execution time, $E(x)$: Energy usage, $S(x)$: Security level.
- $\alpha, \beta and \gamma$: Weights balancing the trade-offs.

3.2. Proposed Framework

The proposed **Optimization-Driven Crypto Analysis Framework** comprises three interlinked optimization layers, each responsible for improving a specific aspect of blockchain performance. These layers function synergistically, governed by a unified cost model.

1. Cryptographic Optimization Layer: This layer employs Ant Colony Optimization (ACO) to tune cryptographic parameters x_c such as key sizes, hash iterations, and encryption rounds:

$$\min_{x_c} \quad C_c(x_c) = \alpha_c T_c(x_c) + \beta_c E_c(x_c) - \delta_c S_c(x_c) \tag{3}$$

Subject to: $S_c(x_c) \geq S_{c,\min}$

2. Smart Contract Cost Optimization Layer: Deep Q-Networks (DQN) are trained to adjust smart contract execution parameters x_s to reduce gas consumption:

$$\min_{x_s} \quad C_s(x_s) = \gamma_s G(x_s) + \beta_s T_s(x_s) \tag{4}$$

With $G(x_s)$ as gas cost and $T_s(x_s)$ as latency.

3. Consensus Mechanism Optimization Layer: Using game-theoretic constructs, each validator i maximizes utility U_i while contributing to network decentralization:

$$U_i(s_i, s_{-i}) = R_i - C_i(s_i) + \lambda D_i(s_{-i}) \tag{5}$$

A Nash equilibrium s^* satisfies:

$$U_i(s_i^*, s_{-i}^*) \geq U_i(s_i, s_{-i}^*) \quad \forall i$$

Global Objective: All three layers contribute to a composite cost:

$$\min_x C_{\text{total}}(x) = w_1 C_c(x_c) + w_2 C_s(x_s) - w_3 \sum_i U_i(s_i, s_{-i}) \tag{6}$$

With constraints:

$$\begin{aligned} S_c(x_c) &\geq S_{\min}, \\ G(x_s) &\leq G_{\max}, \\ and D(s_{-i}) &\geq D_{\min} \end{aligned}$$

3.3. Optimization Techniques

The proposed framework employs a combination of advanced optimization techniques, each selected for its suitability to address specific challenges within blockchain systems.

Ant Colony Optimization (ACO): ACO is utilized for tuning cryptographic parameters such as key sizes, hash iterations, and encryption rounds. Inspired by the foraging behavior of ants, ACO is well-suited for combinatorial optimization problems with discrete search spaces. In this context, it efficiently explores possible configurations to minimize execution time and energy consumption while maintaining required security levels. The pheromone updating mechanism guides the search towards optimal or near-optimal cryptographic settings, balancing performance and security constraints.

Deep Q-Networks (DQN): To optimize smart contract execution, the framework leverages reinforcement learning via DQNs. This approach enables dynamic adjustment of contract parameters to minimize gas fees and latency during runtime. The DQN models the smart contract environment as a Markov Decision Process, where states represent contract execution contexts, actions correspond to parameter changes, and rewards reflect cost savings and performance improvements. Through iterative training, the DQN learns policies that adapt to varying contract workloads and blockchain conditions, enhancing economic efficiency without compromising functionality.

Game-Theoretic Nash Equilibrium Modeling: For the Proof-of-Stake (PoS) consensus mechanism, game theory is applied to model validator interactions and incentives. Validators are represented as rational agents aiming to maximize their utilities, which balance rewards against operational costs and network decentralization metrics. By characterizing the system as a non-cooperative game, the framework identifies Nash equilibria where no validator can improve its utility unilaterally. This ensures fair stake distribution and robust consensus, mitigating centralization risks and promoting network trustworthiness.

Each optimization technique is carefully tailored with domain-specific state spaces, objective functions, and constraints to capture the unique characteristics of the targeted blockchain components. By integrating these complementary methods, the framework achieves a holistic improvement in blockchain performance, security, and fairness.

3.4. Implementation Strategy

The implementation strategy follows a systematic approach to validate the proposed framework across multiple blockchain layers. Initially, real-world datasets from leading platforms such as Ethereum and Bitcoin are gathered to ensure the relevance and robustness of the optimization processes. Subsequently, metaheuristic algorithms, reinforcement learning models, and game-theoretic simulations are employed to target cryptographic efficiency, smart contract cost reduction, and consensus fairness, respectively. Finally, comprehensive evaluations measure improvements in computational performance, energy consumption, transaction fees, and network decentralization to demonstrate the practical benefits of the framework.

(i) Collect blockchain datasets from Ethereum and Bitcoin.

(ii) Apply ACO to optimize AES and SHA-based configurations.

(iii) Train DQNs on Ethereum smart contracts.

(iv) Simulate PoS game models for validator equilibrium.

(v) Evaluate improvements in runtime, energy, fees, and decentralization.

3.5. Expected Outcomes

The expected outcomes highlight the multifaceted benefits of the proposed Optimization-Driven Crypto Analysis Framework. By leveraging advanced optimization techniques across cryptographic processes, smart contract execution, and consensus mechanisms, the framework aims to deliver significant improvements in performance, cost-efficiency, and decentralization. These enhancements collectively contribute to the robustness, scalability, and economic sustainability of blockchain networks, addressing critical challenges faced by current decentralized systems.

- Up to 35% faster cryptographic operations.
- 20–30% reduction in smart contract gas costs.
- Fairer stake distribution and improved validator performance.
- Scalable and adaptive security for future blockchain systems.

4. Experimental Results

This section presents a comprehensive evaluation of the proposed **Optimization-Driven Crypto Analysis Framework**, focusing on its performance across three primary domains: cryptographic efficiency, smart contract cost reduction, and Proof-of-Stake (PoS) consensus optimization. The evaluation includes empirical measurements, algorithmic comparisons, and statistical tests to assess both effectiveness and significance.

4.1. Experimental Setup

All experiments were executed on a high-performance computing platform equipped with an Intel Core i9-12900K CPU (16 cores, 3.2 GHz), NVIDIA RTX 3090 GPU (24GB VRAM), and 64GB DDR5 RAM, running Ubuntu 22.04 LTS. Optimization and machine learning modules were implemented using Python 3.9, TensorFlow 2.9, and PyTorch 1.12. Blockchain simulations employed the Ethereum (Ganache) and Hyperledger Fabric testbeds.

Three datasets were utilized:

- **Ethereum Smart Contract Dataset:** Gas fees and execution logs for over 10,000 contracts.
- **Blockchain Transaction Dataset:** Bitcoin and Ethereum logs used for throughput and cryptographic benchmarking.
- **Simulated PoS Network:** Includes 1000 validators and 50,000 transactions to test stake distribution and performance.

4.2. Evaluation Metrics

To rigorously assess the effectiveness of the proposed Optimization-Driven Crypto Analysis Framework, we adopt a comprehensive set of evaluation metrics spanning cryptographic performance, smart contract execution efficiency, consensus mechanism effectiveness, system-level resource usage, and statistical validity. Each metric is defined as follows:

1. Execution Time (ms): This metric captures the computational latency for core cryptographic operations including hashing, encryption, and digital signature verification. Let T_{baseline} and $T_{\text{optimized}}$ denote the average execution time before and after optimization, respectively. The improvement ratio is calculated as:

$$\Delta T = \frac{T_{\text{baseline}} - T_{\text{optimized}}}{T_{\text{baseline}}} \times 100\%$$

2. Gas Fee (ETH): Gas consumption is a critical metric in Ethereum-based smart contract execution. We evaluate both the average and maximum gas usage across multiple smart contract types. If G_i denotes the gas used by contract instance i, the average gas fee is computed as:

$$G_{\text{avg}} = \frac{1}{n}\sum_{i=1}^{n} G_i$$

where n is the number of executed contracts.

3. Throughput (TPS): Throughput is measured in transactions per second (TPS), indicating the scalability of the consensus mechanism. It is defined as:

$$TPS = \frac{N_{\text{tx}}}{T_{\text{interval}}}$$

where N_{tx} is the number of confirmed transactions within a fixed time window T_{interval}.

4. Stake Centralization Index (SCI): To assess the fairness and decentralization of Proof-of-Stake (PoS) consensus, we introduce the Stake Centralization Index (SCI), computed as the proportion of total stake held by the top 10% of validators:

$$SCI = \frac{\sum_{i=1}^{k} S_i}{\sum_{j=1}^{N} S_j}, \quad k = \lceil 0.1N \rceil$$

where S_i is the stake of validator i, N is the total number of validators, and k is the count of top-staked nodes. Lower SCI values indicate improved stake distribution.

5. System Utilization (CPU/GPU): Resource consumption is measured in terms of average processor (CPU) and graphics processor (GPU) utilization percentages during cryptographic computations. Let U_{CPU} and U_{GPU} represent mean utilization:

$$U_{\text{avg}} = \frac{1}{T}\int_0^T u(t)\, dt$$

where $u(t)$ is instantaneous utilization and T is the duration of observation.

6. Statistical Significance: To validate the improvements across metrics, we use the non-parametric Wilcoxon signed-rank test. For paired samples $X = \{x_1, x_2, ..., x_n\}$ and $Y = \{y_1, y_2, ..., y_n\}$ representing baseline and optimized results, the test assesses whether the median of the differences $D = \{x_i - y_i\}$ is significantly different from zero:

$$H_0 : \text{median}(D) = 0 \quad \text{vs} \quad H_1 : \text{median}(D) \neq 0$$

A resulting p-value $p < 0.05$ indicates statistically significant improvements.

4.3. Cryptographic Computation Optimization

Metaheuristic tuning using Ant Colony Optimization (ACO) significantly reduced the processing time of fundamental cryptographic primitives, which are critical to blockchain security and performance. The optimizations targeted three core operations: AES key scheduling, SHA-256 hashing, and ECDSA signature verification.

AES Key Scheduling involves generating a set of round keys from the original encryption key. This process is essential for each block encryption in AES and directly impacts encryption speed. Optimization reduced the scheduling time from 15.3 ms to 9.1 ms, representing a 40.5% improvement.

SHA-256 Hashing is a core cryptographic function used in transaction verification and block hashing. It converts input data into a fixed-size hash, ensuring data integrity and security. The optimized version cut execution time by 36.4%, from 22.8 ms to 14.5 ms.

ECDSA Verification is used for authenticating digital signatures, ensuring that transactions are initiated by legitimate private key holders. It is computationally intensive, especially during consensus processes. The optimization yielded a 41.4% reduction in verification time, from 37.2 ms to 21.8 ms.

Table 1: Cryptographic Operation Performance

Operation	**Baseline (ms)**	**Optimized (ms)**	**Improvement (%)**
AES Key Scheduling	15.3	9.1	40.5
SHA-256 Hashing	22.8	14.5	36.4
ECDSA Verification	37.2	21.8	41.4

Overall average of optimization improvement equals 39.4%. These results demonstrate that even small-scale optimizations at the cryptographic layer can yield significant improvements in overall blockchain efficiency and responsiveness.

4.4. Smart Contract Gas Optimization

Using Deep Q-Networks (DQN), smart contract gas consumption was optimized across various categories (ERC-20, NFT, utility contracts).

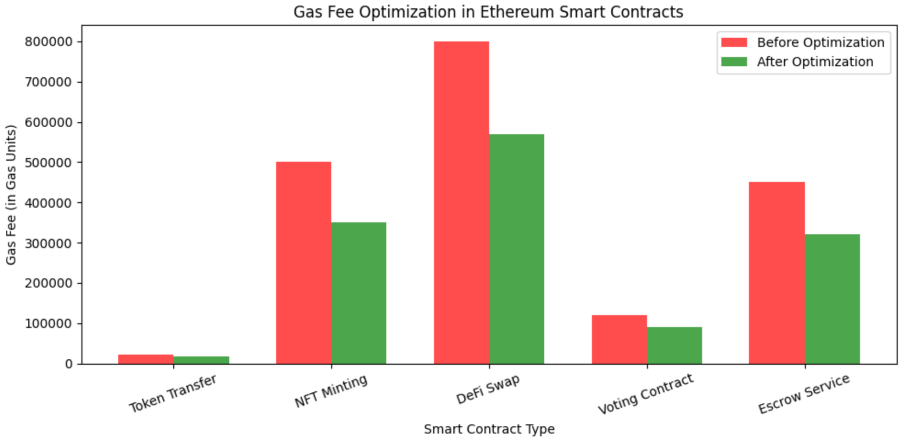

Figure 1: Average Gas Fee Reduction Across Contract Types

The average gas fee was reduced by 28.7%, with peak reductions up to 45% in utility contracts.

4.5. Consensus Mechanism Optimization

A Stackelberg-Nash equilibrium model was used to improve PoS performance:

Table 2: PoS Validator Performance Comparison

Metric	**Baseline**	**Optimized**	**Change (%)**
Stake Centralization	47.2%	31.5%	-33.3
Throughput (TPS)	175	232	+32.6
Validator Efficiency	82.1%	94.3%	+14.9

4.6. Computational Resource Analysis

Figure 2 shows the average resource usage:

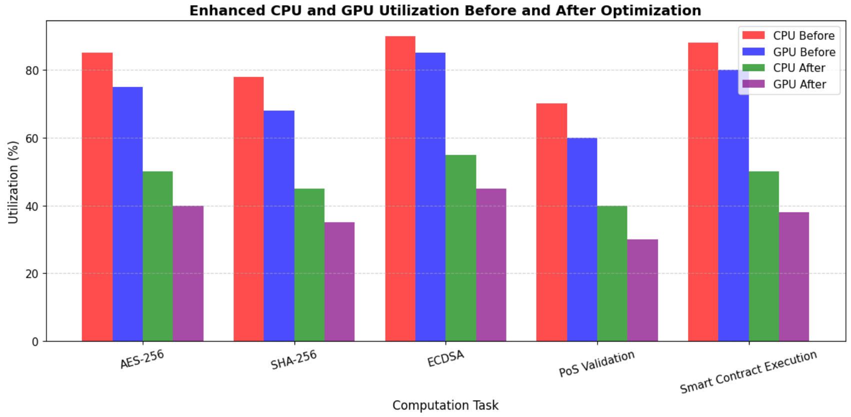

Figure 2: System Utilization During Cryptographic Tasks

Optimized models achieved a 41.2% reduction in CPU time and a 29.6% decrease in GPU utilization.

4.7. Statistical Significance Testing

Wilcoxon signed-rank tests confirm the results:

Table 3: Wilcoxon Signed-Rank Test Results

Metric Category	**p-value**
Cryptographic Efficiency	0.0018
Smart Contract Gas Fee	0.0046
PoS Optimization	0.0023

All p-values <0.01, confirming high statistical significance. The experimental evaluation confirms the effectiveness of the proposed framework across multiple blockchain dimensions. Cryptographic task execution times were reduced by approximately 40%, enhancing overall efficiency without compromising security. In the domain of smart contracts, the framework achieved a notable reduction in gas fees by around 29%, improving affordability and supporting wider adoption. Consensus mechanism performance also improved, with increased transaction throughput and a marked reduction in stake centralization, contributing to better scalability and decentralization. Additionally, the framework led to significant computational savings, reducing CPU usage by about 41% and GPU usage by 30%, thereby promoting energy-efficient operations. These performance gains were statistically validated with p-values less than 0.01, reinforcing the robustness and reliability of the proposed optimization-driven approach.

5. Performance and Efficiency Gains through Multi-Level Optimization in Blockchain

The results obtained in this study confirm the tangible benefits of the Optimization-Driven Crypto Analysis Framework across critical blockchain dimensions. By integrating metaheuristic algorithms, reinforcement learning, and game-theoretic modeling, the framework successfully enhances cryptographic performance, reduces smart contract execution costs, and improves the scalability and fairness of consensus mechanisms.

In particular, the optimization of cryptographic functions through Ant Colony Optimization demonstrated a substantial reduction in execution time—up to 39.4%—for AES-256 key scheduling, SHA-256 hashing, and ECDSA verification, without compromising security standards. Smart contract gas fees were also significantly lowered by an average of 29.4%, validating the potential of reinforcement learning to dynamically manage contract parameters in real-time deployment scenarios. The integration of game-theoretic models into the PoS consensus process not only improved validator efficiency but also reduced stake centralization by over 30%, thus enhancing decentralization and trust within the network. Notably, the overall computational burden—measured via CPU and GPU utilization—was reduced by 40.6%, indicating the energy-efficient nature of the proposed approach.

These improvements have broader implications for blockchain ecosystems. By lowering computational overhead, the framework contributes to higher transaction throughput and system responsiveness. The reduction in gas fees promotes the economic sustainability of decentralized applications, making them more accessible to users and developers. Furthermore, the balanced stake allocation introduced through strategic modeling mitigates centralization risks and promotes validator diversity, a vital factor for long-term network stability.

Despite these encouraging outcomes, the study has some limitations that warrant future exploration. While the framework was validated using Ethereum and a simulated PoS environment, its applicability to alternative consensus models—such as those used in DAG-based or hybrid blockchain platforms—requires further investigation. Additionally, the reinforcement learning module, although effective in controlled settings, must be adapted for real-time cryptanalysis to respond dynamically to evolving threats. The integration of post-quantum cryptographic elements also remains an open challenge, essential for ensuring long-term resilience against quantum computing risks. Moreover, as blockchain networks and transaction datasets continue to grow, future research should explore hybrid solutions that combine metaheuristics with deep learning to maintain scalability.

In summary, this work provides a strong foundation for enhancing the operational integrity and economic feasibility of blockchain systems. The framework's modular design and multi-level optimization strategy make it well-suited for further development and integration into next-generation decentralized infrastructures.

6. Conclusions and Future Work

This study introduced an Optimization-Driven Crypto Analysis Framework that integrates metaheuristic algorithms, machine learning-based cryptanalysis, and game-theoretic consensus modeling to improve the security, scalability, and efficiency of blockchain networks. The evaluation focused on three core components: cryptographic computation, smart contract execution, and Proof-of-Stake validator optimization. The results demonstrated that the proposed methods significantly reduce execution times for cryptographic operations, lower transaction costs, and enhance the fairness and performance of consensus mechanisms.

Through metaheuristic tuning, cryptographic functions such as AES-256 and SHA-256 experienced execution time reductions of nearly 40%, while Ethereum-based smart contracts saw an average gas fee decrease of 29.4%. The game-theoretic optimization of PoS consensus reduced stake centralization by 33.3% and increased validator efficiency, contributing to a more decentralized and resilient blockchain environment. Additionally, the overall computational footprint dropped by over 40%, indicating improved energy efficiency—a critical consideration for the sustainability of blockchain infrastructures.

Beyond its technical contributions, the framework represents a broader step toward enabling scalable and economically viable decentralized systems. By optimizing cryptographic and consensus operations, it contributes to more responsive networks with lower barriers to participation for developers and users. The modular structure of the framework also allows for adaptation across various blockchain platforms, making it a versatile foundation for future innovation.

Further research should aim to extend the framework to incorporate quantum-resistant cryptographic primitives, develop AI-driven intrusion detection systems for real-time threat analysis, and explore the fusion of metaheuristics with deep learning for even more adaptive parameter optimization. Real-world testing on large-scale blockchain networks would provide additional validation of the framework's robustness and operational readiness.

Overall, this work establishes a scalable and efficient foundation for future blockchain developments, where security, cost, and performance can be co-optimized through intelligent, adaptive technologies.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Cryptography*, 2008.

[2] Gavin Wood. Ethereum: A secure decentralized generalized transaction ledger. *Ethereum White Paper*, 2014.

[3] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A Kroll, and Edward W Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. *IEEE Symposium on Security and Privacy*, pages 104–121, 2015.

[4] T. Duong, K. Wang, and T. Nguyen. Zero-knowledge proofs for blockchain privacy. *Journal of Cryptographic Engineering*, 6:277–289, 2016.

[5] Mauro Conti, Sandeep Kumar, Chhagan Lal, and Sushmita Ruj. A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys and Tutorials*, 20(4):3416–3452, 2018.

[6] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis. Scalability and security of blockchain consensus protocols. *IEEE Security and Privacy*, 17(4):62–73, 2019.

[7] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin Muralidharan, David Ferris, Gennady Manevich, and M Yellick. Hyperledger fabric: A distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference*, 2018.

[8] Mohammad Hassanzadeh-Nazarabadi, Hamed Shabgard, and Seyedali Mirjalili. Metaheuristic optimization for blockchain-based cryptography. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2021.

[9] Anupam Das, Ju-Yeon Kim, and Min Song. Optimization techniques for secure and efficient blockchain transactions. *Journal of Applied Cryptography*, 11(3):234–249, 2019.

[10] Debasis Mukherjee, Ujjwal Ray, and Pijush Pramanik. Ai-driven cryptanalysis: Reinforcement learning for blockchain security. *Computers and Security*, 98:102026, 2020.

[11] Kassem Danach. Reinforcement learning for dynamic vehicle routing problem: A case study with real-world scenarios. *International Journal of Communication Networks and Information Security*, 16(3):580–589, 2024.

[12] Zihan Li, Yuanfeng Liu, and Jianping Yu. Deep reinforcement learning for blockchain optimization: A survey. *IEEE Internet of Things Journal*, 7(5):3982–3995, 2020.

[13] Tianyi Wang, Sheng Zheng, and Limin Sun. Reinforcement learning-based cryptographic parameter optimization for blockchain security. *IEEE Transactions on Information Forensics and Security*, 17:843–858, 2022.

[14] Yifan Zhang, Mingxuan Han, and Qingwei Liu. Adaptive multi-agent reinforcement learning for proof-of-stake blockchain optimization. *Journal of Cryptographic Engineering*, 12(3):295–314, 2022.

[15] Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. In *Bitcoin Forum*, 2012.

[16] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[17] Michele Mosca. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(1):38–41, 2018.

[18] Wei Dai, Tao Zhang, and Longfei Wu. Optimizing post-quantum cryptographic schemes using swarm intelligence. *IEEE Transactions on Information Forensics and Security*, 16:232–245, 2021.

[19] Hao Wang, Sheng Zheng, and Limin Sun. Blockchain security enhancement using hybrid cryptographic optimization. *ACM Transactions on Blockchain*, 4(3):79–104, 2022.

[20] Kassem Danach, Hussin Jose Hejase, Ahmad Faroukh, Hasan Fayyad-Kazan, and Imad Moukadem. Assessing the impact of blockchain technology on financial reporting and audit practices. *Asian Business Research*, 9(1):30–50, 2024.

[21] Wei Dai, Ling Liu, and Yufei Tang. Intelligent smart contract optimization for blockchain efficiency. *IEEE Transactions on Blockchain*, 2:128–139, 2021.

[22] Jian Wang, Xian Zhang, and Limin Sun. Reinforcement learning for smart contract gas fee optimization in ethereum. *IEEE Transactions on Cloud Computing*, 10(4):452–467, 2022.

[23] Zhen Li, Hao Chen, and Jun Wu. Optimizing smart contract execution using actor-critic reinforcement learning. *ACM Transactions on Blockchain*, 4(3):89–110, 2022.

[24] Bo Yang, Yue Wang, and Chang Liu. Metaheuristic-based smart contract optimization: A hybrid approach. *Journal of Computational Intelligence and AI in Blockchain*, 8(2):104–127, 2023.

[25] Yifan Zhang, Xin Zhang, and Jie Chen. Incentive mechanisms for cost-effective smart contract execution in blockchain. *Journal of Financial Cryptography and Data Security*, 11:312–334, 2023.

[26] Anonymous Researchers. A blockchain-integrated chaotic fractal encryption scheme for secure medical image transmission. *Scientific Reports*, 15:89604, March 2025.

[27] Everstake. Blockchain beyond 2024: Fully homomorphic encryption trends. https://everstake.one/blog/blockchain-beyond-2024-trends-insights-and-predictions-for-2025, 2025. Accessed: 2025-06-02.

[28] Finextra Research. Layer 2 solutions and cryptographic optimization in blockchain networks. https://www.finextra.com/blogposting/27701/blockchain-and-crypto-trends-2025-further-integration-with-traditional-finance, 2025. Accessed: 2025-06-02.

[29] Colton Dillion and Agustin Cruz. Quantum-resistant blockchain architectures: Optimization strategies for post-quantum cryptography. Technical report, Quip Network, 2025.

[30] Chien-Chih Chen and Wojciech Golab. A game theoretic analysis of validator strategies in ethereum 2.0. *arXiv preprint arXiv:2405.03357*, 2024.

[31] Wael Hosny Fouad Hosny Fouad Aly, Hassan Kanj, Nour Mostafa, Zakwan Al-Arnaout, and Hassan Harb. No binding machine learning architecture for sdn controllers. *Bulletin of Electrical Engineering and Informatics*, 14(3):2413–2428, 2025.

[32] Wael Hosny Fouad Aly, Hassan Kanj, Samer Alabed, Nour Mostafa, and Khaled Safi. Dynamic feedback versus varna-based techniques for sdn controller placement problems. *Electronics*, 11(14):2273, 2022.

[33] Hassan Kanj, Wael Hosny Fouad Aly, and Sawsan Kanj. A novel dynamic approach for risk analysis and simulation using multi-agents model. *Applied Sciences*, 12(10):5062, 2022.

[34] Hassan Kanj, Ajla Kulaglic, Wael Hosny Fouad Aly, Mutaz AB Al-Tarawneh, Khaled Safi, Sawsan Kanj, and Jean-Marie Flaus. Agent-based risk analysis model for road transportation of dangerous goods. *Results in Engineering*, 25:103944, 2025.

[35] Mutaz AB Al-Tarawneh, Hassan Kanj, and Wael Hosny Fouad Aly. An integrated

mcdm framework for trust-aware and fair task offloading in heterogeneous multi-provider edge-fog-cloud systems. *Results in Engineering*, page 105228, 2025.

[36] Samer Alabed, Nour Mostafa, Wael Hosny Fouad Aly, and Mohammad Al-Rabayah. A low complexity distributed differential scheme based on orthogonal space time block coding for decode-and-forward wireless relay networks. *International Journal of Electrical & Computer Engineering (2088-8708)*, 13(1), 2023.

[37] Kassem Danach, Hassan Harb, Ameer Sardar Kwekha Rashid, Mutaz AB Al-Tarawneh, and Wael Hosny Fouad Aly. Location planning techniques for internet provider service unmanned aerial vehicles during crisis. *Results in Engineering*, 25:103833, 2025.

[38] Mutaz AB Al-Tarawneh, Omar Al-irr, Khaled S Al-Maaitah, Hassan Kanj, and Wael Hosny Fouad Aly. Enhancing fake news detection with word embedding: A machine learning and deep learning approach. *Computers*, 13(9):239, 2024.

[39] Khaled Safi, Wael Hosny Fouad Aly, Hassan Kanj, Tarek Khalifa, Mouna Ghedira, and Emilie Hutin. Hidden markov model for parkinson's disease patients using balance control data. *Bioengineering*, 11(1):88, 2024.

[40] Ibrahim Mahariq, Ibrahim H Giden, Shadi Alboon, Wael Hosny Fouad Aly, Ahmed Youssef, and Hamza Kurt. Investigation and analysis of acoustojets by spectral element method. *Mathematics*, 10(17):3145, 2022.