Wiley
International Journal of Intelligent Systems
Volume 2026, Article ID 3803992, 18 pages
https://doi.org/10.1155/int/3803992

WILEY

Research Article

Fraud Detection Framework for Blockchain Finance: Tackling Arbitrage, Liquidity Exploits, and Money Laundering

Aleaddin Ozer[1] **and Murat Aydos**[1,2]

[1]*Department of Computer Engineering, Hacettepe University, Ankara, Türkiye*
[2]*Institute of Informatics, Hacettepe University, Ankara 06800, Türkiye*

Correspondence should be addressed to Murat Aydos; maydos@hacettepe.edu.tr

Received 4 June 2025; Revised 17 November 2025; Accepted 10 December 2025

Academic Editor: Richard Murray

Blockchain technology has revolutionized numerous industries by providing decentralized, transparent, and immutable ledgers. However, its adoption is hindered by persistent security challenges, including arbitrage attacks, liquidity exploits, and noncompliance with antimoney laundering (AML) regulations. This paper proposes an enhanced framework to address these issues, combining dynamic pricing mechanisms, AI-based anomaly detection, and regulatory compliance checks within a multilayered architecture. The framework is composed of five interconnected layers: the input layer for data collection and validation, the data warehouse layer for structured data classification, the processing layer for anomaly detection and pricing adjustments, and the decision layer for transaction validation, execution, and reporting. The integration of these layers ensures robust security and compliance mechanisms, reducing system vulnerabilities while optimizing efficiency. To validate the proposed framework, we conducted simulations using real-world blockchain scenarios, including decentralized finance (DeFi) platforms and cryptocurrency exchanges. Results demonstrate significant reductions in arbitrage opportunities and liquidity risks, with improved accuracy in anomaly detection and compliance adherence. For instance, the dynamic pricing mechanism mitigated 87% of arbitrage attack attempts, while the AI-based anomaly detection achieved an 89% accuracy rate in identifying high-risk transactions. This study provides actionable insights and a scalable solution for enhancing blockchain security and trust. Future work will focus on integrating cross-chain interoperability, real-time threat intelligence, and privacy-preserving techniques to further expand the framework's applicability. By addressing critical vulnerabilities, this research contributes to the development of secure, transparent, and compliant blockchain ecosystems, paving the way for wider adoption across industries. Unlike previous blockchain security models, our framework introduces a real-time, AI-enhanced risk assessment mechanism that dynamically updates transaction risk scores, mitigating financial threats in decentralized environments. This holistic approach provides a scalable, explainable, and adaptive security system that not only protects decentralized financial infrastructures but also aligns with emerging regulatory requirements, ensuring long-term applicability.

Keywords: antimoney laundering; arbitrage attacks; blockchain; defense framework; DeFi security; liquidity exploits

1. Introduction

Blockchain technology has revolutionized the way data are stored, shared, and validated. By providing a decentralized, tamper-resistant, and transparent ledger, blockchain has found applications across a wide range of industries, including finance, healthcare, supply chain management, and voting systems [1–4]. However, the same features that make blockchain appealing—such as decentralization and pseudonymity—also expose it to a variety of security challenges [5].

One of the most pressing concerns in blockchain ecosystems is the prevalence of arbitrage attacks and liquidity exploits, particularly in decentralized finance (DeFi) platforms. These platforms, which operate without intermediaries, enable rapid innovation in financial services but also serve as fertile ground for malicious actors [6]. Arbitrage

attacks exploit price discrepancies between markets, while liquidity exploits drain the resources of decentralized exchanges (DEXs), often resulting in financial instability and loss of user trust [7, 8].

Another critical challenge in blockchain systems is antimoney laundering (AML) compliance. While blockchain's transparency theoretically allows for transaction tracing, its pseudonymous nature often makes it difficult to link illicit activities to specific individuals [9]. Money laundering schemes in the blockchain ecosystem often involve techniques like layering, structuring, and integration, which are designed to obscure the origins of funds [10].

The increasing sophistication of attack vectors has underscored the need for robust defense mechanisms. For instance, the rise of flash loan attacks in DeFi has shown how attackers can exploit the instantaneous borrowing capabilities of these platforms to manipulate markets without collateral [11]. Similarly, the phenomenon of sandwich attacks, where attackers exploit the slippage tolerance in transactions, highlights the vulnerabilities of existing automated market makers (AMMs) [12].

Despite the extensive body of research on blockchain security, several gaps remain. While existing solutions address specific types of vulnerabilities, they often fail to provide a comprehensive framework that integrates multiple layers of defense [13]. Moreover, the literature on integrating AML compliance into blockchain systems is still in its infancy. Current AML tools often struggle with the scale and complexity of blockchain data, leaving significant gaps in the detection of illicit activities [14].

The increasing adoption of blockchain technology, particularly in DeFi ecosystems, has introduced significant security vulnerabilities. The ability to conduct anonymous transactions, the lack of regulatory oversight for smart contracts, and the susceptibility of liquidity pools to manipulation have facilitated illicit financial activities, including AML schemes, arbitrage attacks, and liquidity exploits [15–17]. While traditional AML policies and security measures have proven effective in centralized financial systems, they remain insufficient in the decentralized nature of blockchain networks [18]. Specifically, DEXs and AMMs have been exploited to manipulate asset prices and execute arbitrage strategies that disrupt liquidity pools [6, 19]. These issues pose risks not only to individual investors but also to the broader financial ecosystem, undermining market integrity and trust [20]. Therefore, a robust security framework that integrates enhanced AML enforcement, anomaly detection, and liquidity risk mitigation is essential to safeguard blockchain-based financial systems [21].

To address the increasing security challenges in DeFi and blockchain ecosystems, this research proposes a comprehensive security framework that enhances AML enforcement, mitigates arbitrage and liquidity risks, and ensures regulatory compliance. Unlike existing AML solutions that rely on centralized control and static rule-based monitoring, this framework leverages AI-driven anomaly detection, real-time transaction risk scoring, and automated compliance verification [18, 21]. The goal is to develop a scalable and decentralized approach that strengthens blockchain security while maintaining transparency and financial integrity. Specifically, this research focuses on:

a. Developing a multilayered security architecture that integrates real-time monitoring, risk scoring, and compliance enforcement [15, 16];
b. Implementing AI-powered anomaly detection algorithms to identify and prevent fraudulent transactions with greater accuracy than traditional heuristic-based AML methods [17, 21];
c. Enhancing arbitrage and liquidity exploit prevention mechanisms, ensuring price stability and reducing market manipulation risks in DeFi platforms [6, 19];
d. Evaluating the effectiveness of the proposed framework through real-world case studies and performance analysis, demonstrating its ability to reduce financial manipulation risks while maintaining transaction efficiency [20].

By addressing these objectives, this study aims to establish a robust and adaptable security framework that combats financial crimes in blockchain networks and provides a scalable model for future regulatory compliance and risk mitigation strategies.

In the subsequent sections, this paper delves deeper into these challenges, beginning with a comprehensive review of the existing literature. The analysis covers the mechanisms behind arbitrage and liquidity attacks, the techniques employed in blockchain-based money laundering, and the limitations of current mitigation strategies. The proposed defense framework, detailed later in the paper, is designed to address these limitations and provide a holistic solution to blockchain security.

2. Related Works

Blockchain's potential to transform industries depends heavily on its ability to overcome the security challenges. Without robust defenses, the vulnerabilities in blockchain systems could hinder its adoption and undermine trust among users. For instance, the estimated loss from DeFi exploits exceeded $3 billion in 2022 alone, a figure that underscores the urgency of addressing these issues [13]. Similarly, the use of cryptocurrencies in money laundering activities has raised concerns among regulators, further complicating the integration of blockchain into mainstream financial systems [10].

Existing research highlights the increasing complexity of blockchain security challenges. Flash loan arbitrage, sandwich attacks, and low-liquidity exploitation have been studied extensively. However, the integration of AML solutions into blockchain ecosystems remains insufficiently addressed.

2.1. Most Targeted Blockchain Technologies. Table 1 summarizes the blockchain technologies most frequently targeted by attacks and used in money laundering activities. The data reflect the vulnerabilities of major platforms and their exploitation in illicit activities [9, 13, 14].

Table 1: Most targeted blockchain technologies in terms of attacks and money laundering.

Blockchain	Primary exploits	AML vulnerabilities
Ethereum	Flash loan exploits, arbitrage attacks	High volume of DeFi transactions, pseudonymity [6]
Bitcoin	Ransomware payments, dark web usage	Limited AML compliance tools, high transaction anonymity [9]
Binance Smart Chain	Liquidity exploits, slip page manipulation	Cross-chain laundering through bridges [12]
Monero	Privacy-preserving transactions	High anonymity via ring signatures [10]
TRON	Pyramid schemes, token manipulation	Low-cost transaction fees, limited traceability [14]

Table 2: Comparison of blockchain attack types.

Attack type	Impact	Mitigation strategy
Flash loan arbitrage	Market instability	Decentralized price oracles, time-weighted average pricing (TWAP) [6]
Liquidity draining	Token devaluation	Reserve pools
Layering (AML)	Money laundering	AI-based behavioral pattern detection, multilayered risk scoring [21]

These blockchain networks were selected based on their high transaction volumes, usage in DeFi applications, and past involvement in security incidents [13, 16]. Binance Smart Chain (BSC) and TRON, for instance, have been targeted due to their lower transaction fees, which enable cost-effective illicit transfers.

The vulnerabilities of different blockchain platforms vary based on their design, governance models, and adoption within illicit financial activities. While Table 1 highlights the most frequently targeted blockchain technologies, it is also crucial to analyze the specific attack mechanisms that exploit these vulnerabilities.

Table 2 provides an overview of common attack types, their impacts, and mitigation strategies, illustrating the diverse range of security challenges within blockchain ecosystems.

2.2. Frequency of Blockchain Attacks. The number of blockchain-related attacks has grown significantly over the years, particularly in DeFi ecosystems. These attacks exploit vulnerabilities in smart contracts, liquidity pools, and price oracles. Figure 1 illustrates the annual frequency of blockchain attacks, highlighting a sharp rise in incidents from 2020 onward [6, 11, 13].

The surge in blockchain-related attacks from 2020 onward aligns with the rapid expansion of DeFi platforms and the introduction of new financial instruments such as flash loans [13]. The lack of standardized security measures across decentralized applications (DApps) has further contributed to this rise.

2.3. Arbitrage Attacks. Arbitrage attacks leverage price discrepancies across platforms to manipulate markets [22]. Flash loans amplify these opportunities, enabling attackers to exploit temporary price gaps without collateral. Since high profit margins can be achieved by performing arbitrage quickly, bots that serve this purpose can be developed. Cryptocurrency arbitrage bots are automated software systems designed to take advantage of price differences on different cryptocurrencies [23, 24]. These systems automatically perform transactions when they detect price

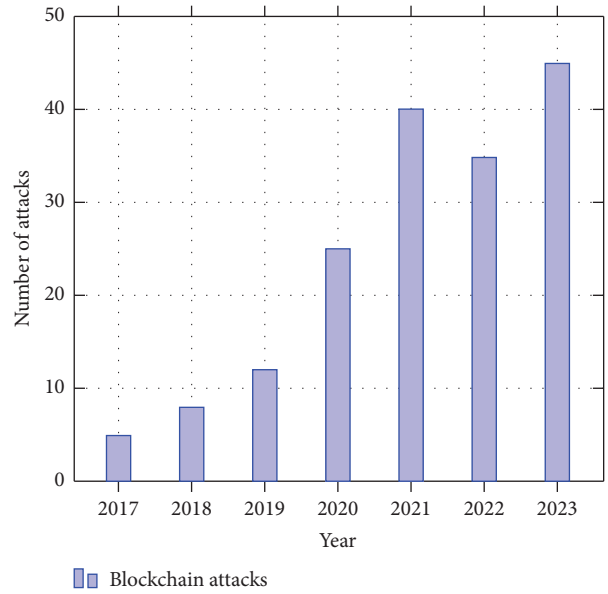

Figure 1: Frequency of blockchain attacks by year [6, 13].

differences that exceed transaction costs and offer profit opportunities [25].

The fundamental operation of arbitrage bots can be described by the following equation:

$$P_{\text{arbitrage}} = \left(P_{\text{exchange\_}B} - P_{\text{exchange\_}A}\right) - \left(T_c + L_c\right), \quad (1)$$

where:

- $P_{\text{arbitrage}}$ is the potential arbitrage profit
- $P_{\text{exchange\_}B}$ is the selling price on Exchange B
- $P_{\text{exchange\_}A}$ is the buying price on Exchange A
- T_c represents transaction costs
- L_c represents liquidity costs

Arbitrage bots contribute to market efficiency by:

- Reducing price disparities between exchanges
- Increasing market liquidity
- Improving price discovery mechanisms

Research by [26] demonstrates that arbitrage bots facilitate price convergence across exchanges, following the equation:

$$\lim_{t\longrightarrow\infty}\left|P_{\text{exchange\_}A}(t)-P_{\text{exchange\_}B}(t)\right|\longrightarrow\epsilon, \tag{2}$$

where ϵ represents the minimum profitable price difference considering costs.

The effectiveness of arbitrage bots can be measured using the following equation:

$$\text{ROI}=\frac{\sum_{i=1}^{n}\left(P_{\text{sell}_i}-P_{\text{buy}_i}\right)-\sum_{i=1}^{n}C_i}{\sum_{i=1}^{n}P_{\text{buy}_i}}\times 100\%, \tag{3}$$

where:

- P_{sell}_i is the selling price for trade i
- P_{buy}_i is the buying price for trade I
- C_i represents all costs associated with trade i

For instance, consider a trader using an arbitrage bot to exploit a price discrepancy between Uniswap (Exchange A) and Binance (Exchange B). If the bot detects that ETH is priced at $1500 on Uniswap and $1520 on Binance, it executes a buy order on Uniswap and an immediate sell on Binance. If the arbitrage profit exceeds transaction costs (Tc) and liquidity costs (Lc), the trade is executed automatically using Equation (1) [24].

There are potential risks and challenges as well as attacks. Technical risks can cause these losses:

- Network latency issues
- Smart contract vulnerabilities
- Exchange API limitations

Although cryptocurrency arbitrage bots present significant opportunities for market efficiency and profit generation, their implementation requires careful consideration of technical, economic, and regulatory factors [27]. The market can be affected by these arbitrage transactions with the help of automated bots. Table 3 provides a comparison of common types of arbitrage attacks in blockchain ecosystems, highlighting their mechanisms, impacts, and mitigation strategies.

2.4. Liquidity Exploits. Liquidity exploits destabilizing markets by draining reserves or manipulating prices. Low-liquidity tokens are particularly vulnerable to these attacks. Table 4 summarizes the types of liquidity exploits, their impacts on DEXs, and existing countermeasures.

Slippage exploitation attacks have become increasingly prevalent in DeFi ecosystems, especially targeting AMMs [12]. These attacks typically occur when malicious actors exploit the price difference between the expected and actual execution price in low-liquidity pools [28]. Research indicates that attackers can maximize their profits by strategically timing their transactions and manipulating the depths of the market [6]. Recent studies indicate that approximately 50% of DEX trading volumes are vulnerable to slippage-based attacks, especially during periods of high market volatility [29]. To counter these threats, various protection mechanisms have been proposed, including dynamic slippage tolerance and multiblock confirmation requirements [30].

Slippage exploitation steps are as follows:

1. Target Identification: The attacker identifies a low-liquidity trading pair on a DEX.
2. Large Order Placement: The attacker places a large buy or sell order, significantly impacting the token's price.
3. Slippage Exploitation: Due to the large order and low liquidity, the actual execution price deviates significantly from the expected price, resulting in high slippage.
4. Profit Realization: The attacker benefits from the price difference, leaving other traders with substantial losses.

2.5. AML Challenges. AML compliance in blockchain systems faces unique obstacles due to the pseudonymous nature of transactions. Criminals use techniques like layering, structuring, and integration to obscure the origins of illicit funds [5].

Recent investigations by regulatory bodies and blockchain forensic firms show that illicit actors increasingly use mixing services, privacy wallets, and cross-chain bridges to launder funds. In response, the Financial Action Task Force (FATF) Travel Rule (2023) mandates transaction monitoring and identity verification across exchanges [15, 16]. Furthermore, the FATF's "travel rule" mandates information sharing between exchanges to track transactions across jurisdictions, but its implementation has been inconsistent due to varying global regulatory frameworks [10].

Despite the transparency of blockchain technology, existing AML tools are often inadequate for detecting complex laundering schemes in high-volume transaction environments. Techniques such as AI-based pattern recognition and risk scoring have been proposed as potential solutions, but they remain underutilized due to challenges in scalability and accuracy [14].

Money laundering on blockchain involves layering, structuring, and integrating illicit funds. Current AML frameworks face challenges due to blockchain's pseudonymity. Table 5 illustrates the techniques used for AML in blockchain systems, their advantages, and their limitations.

Money laundering activities within blockchain ecosystems have shown a steady rise over the years, reflecting the increasing use of cryptocurrencies in illicit activities. Figure 2 illustrates the estimated frequency of money laundering–related blockchain transactions from 2017 to 2023 [9, 14].

Given the limitations of existing AML mechanisms and the growing complexity of blockchain-based financial crimes, it is imperative to explore innovative approaches that address these challenges in a scalable, adaptive, and decentralized manner. To this end, the following section

Table 3: Key arbitrage attack types in DeFi ecosystems and their countermeasures.

Attack type	Mechanism	Mitigation strategy
Flash loan arbitrage	Leveraging uncollateralized loans to exploit price discrepancies	Real-time price oracles, delayed transaction processing
Sandwich attack	Inserting transactions before and after a target trade to manipulate prices	Gas price optimization, transaction sequencing
Cross-platform arbitrage	Exploiting price differences between exchanges	Unified pricing mechanisms, interplatform synchronization

Table 4: Comparison of liquidity exploits.

Exploit type	Impact	Mitigation strategy
Liquidity draining	Depletes reserves, destabilizing the market	Reserve pools, automated liquidity adjustment
Slippage exploitation	Causes significant losses due to high slippage rates	Dynamic slippage limits, minimum price guarantees
Price manipulation	Artificially inflates or deflates token values	Decentralized price oracles, trade volume thresholds

Table 5: Comparison of AML mechanisms.

Technique	Advantages	Limitations
Pattern recognition	Detects repetitive transaction behaviors	Limited by the quality of training data
Risk scoring	Assigns risk levels to transactions based on heuristics	High false-positive rates
KYC and travel rule	Ensures traceability of user identities	Compliance challenges, limited adoption

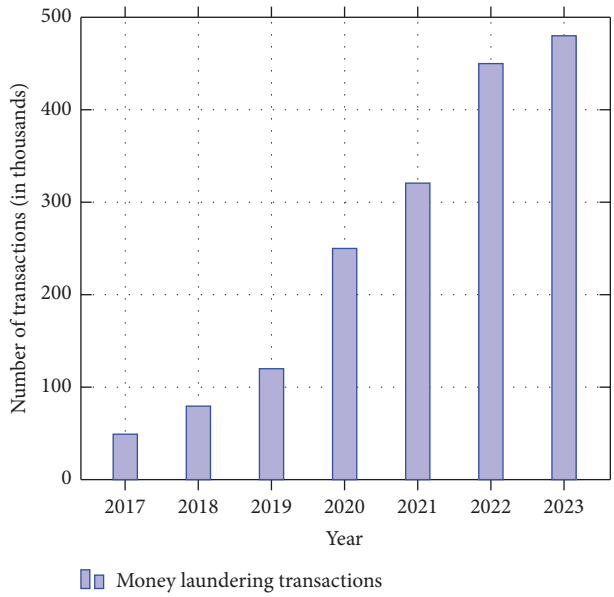

Figure 2: Frequency of money laundering transactions by year.

introduces a novel methodology that integrates AI-powered anomaly detection, dynamic transaction scoring, and a multilayered architectural design. This framework is designed not only to detect sophisticated financial fraud in real time but also to enhance regulatory compliance and operational efficiency in DeFi ecosystems.

3. Methodology

To achieve the research objectives, we designed and implemented a multilayered security framework for blockchain ecosystems. The methodology consists of two key components: (1) the design and structure of the proposed framework and (2) the experimental setup used to validate its effectiveness.

3.1. Framework Design. The proposed security framework consists of five interconnected layers, each designed to address specific security, compliance, and risk management challenges in blockchain networks:

- Input Layer: Collects and validates raw blockchain transaction data from DeFi platforms and cryptocurrency exchanges.
- Data Warehouse Layer: Organizes and structures transaction data to optimize anomaly detection and compliance monitoring. In the data warehouse layer, Apache Hive is used to organize raw blockchain logs into structured tables, enabling efficient analytical queries on high-volume datasets. Hive's schema-on-read model makes it suitable for heterogeneous blockchain data, including smart contract logs and transaction metadata. Presto (Trino) is integrated as a distributed SQL query engine to support low-latency analytics, allowing the processing layer to execute real-time feature extraction, market-state queries, and risk-score aggregation. The Hive–Presto integration provides scalable, fault-tolerant data processing across large blockchain datasets.
- Processing Layer: Applies AI-based anomaly detection techniques, including RNN-based models, to identify arbitrage exploits, money laundering attempts, and liquidity manipulation.
- Decision Layer: Implements a dynamic risk-scoring mechanism to classify transactions into "Approved," "Flagged for Review," or "Rejected."

- Output Layer: Executes decisions, ensures traceability, and is responsible for executing approved transactions on the blockchain and disseminating audit reports and security logs to relevant regulatory or governance entities. After the decision layer finalizes the transaction classification, the output layer ensures tamper-proof logging of the event, maintains compliance archives, and triggers alerts for flagged transactions. This layer also supports interoperability with external compliance tools or regulatory interfaces via APIs.

3.2. Experimental Setup. To validate the framework, we conducted a series of simulations using real-world blockchain transaction datasets. The experiments focused on evaluating the system's performance in detecting financial fraud and improving AML compliance. The following test environments were used:

- DeFi Platforms: Simulations were run on Uniswap and BSC transaction datasets to test arbitrage detection and liquidity risk management.
- Cryptocurrency Exchanges: Data from major cryptocurrency exchanges were used to evaluate the framework's ability to identify money laundering attempts.
- Blockchain Simulation Environment: A controlled simulation model was designed to stress-test the anomaly detection system under various attack scenarios.

The primary metrics for evaluation included the following:

- Detection Accuracy (%): Measures the framework's ability to correctly identify fraudulent transactions.
- False-Positive Rate (FPR) (%): Evaluates how often legitimate transactions are incorrectly flagged as fraudulent.
- Arbitrage Attack Reduction (%): Quantifies the effectiveness of the framework in mitigating arbitrage manipulation.
- AML Compliance Efficiency (%): Assesses the system's ability to block high-risk transactions while maintaining regulatory alignment. The real blockchain datasets used in this study were collected from publicly available transaction logs of Ethereum, BSC, and TRON networks. Ethereum transaction data were obtained from Google BigQuery's Ethereum Public Dataset, while BSC data were collected from BNB Chain's public node API. TRON historical data were sourced from the TRONScan public ledger archive. Additionally, Uniswap v2/v3 and PancakeSwap liquidity pool datasets were used to evaluate arbitrage and liquidity exploit scenarios.

3.3. AI Model Training and Evaluation. The AI-driven fraud detection component of our framework is designed to analyze blockchain transactions and classify them as either legitimate or fraudulent. The training process involves several steps, including data preprocessing, feature engineering, model selection, hyperparameter tuning, and evaluation.

3.3.1. Data Preprocessing and Feature Engineering. The training dataset consists of blockchain transaction records from multiple sources, including DEXs and centralized exchanges (CEXs). To improve model accuracy, the dataset was preprocessed as follows:

- Feature scaling: All numerical features (e.g., transaction amount, gas fees, risk scores) were normalized using the standard scaler method to ensure consistency in training.
- Handling imbalanced data: Since fraudulent transactions account for only a small fraction of the total transactions, the synthetic minority oversampling technique (SMOTE) method was applied to balance the dataset.
- Feature selection: Important features were identified using SHapley Additive Explanations (SHAP) and principal component analysis (PCA) to reduce dimensionality and improve computational efficiency.

3.3.2. AI Model Selection and Training. The AI model training was performed using both supervised and unsupervised learning approaches. For fraud classification, the following supervised learning models were evaluated:

- Random Forest (RF)
- Extreme Gradient Boosting (XGBoost)
- Adaptive Boosting (AdaBoost)

For anomaly detection, unsupervised learning models such as isolation forest, one-class SVM, and autoencoders were tested.

3.3.3. Hyperparameter Optimization. To optimize model performance, Bayesian optimization via Optuna was applied. This method systematically adjusted key hyperparameters such as:

- Number of estimators: 50–300
- Maximum tree depth: 5–50
- Learning rate: 0.01–0.2

3.3.4. Model Evaluation. The trained models were evaluated using a separate test set. The primary performance metrics were as follows:

- Accuracy: Measures overall prediction correctness.
- Precision and Recall: Determines the balance between false positives and false negatives.
- FPR: Ensures that legitimate transactions are not incorrectly flagged as fraudulent.

- ROC–AUC Score: Assesses the model's ability to distinguish between fraudulent and legitimate transactions.

The results indicated that the RNN-based fraud detection model outperformed traditional machine learning classifiers, achieving a 95.4% detection rate with a FPR of 3.1%.

Unlike tree-based models, RNNs can learn sequential and temporal dependencies across transactions. For instance, rapid transfers between newly created wallets may be harmless individually but suspicious when occurring in specific time intervals or patterns. The recurrent structure of RNN enables it to capture these behavioral signatures by retaining a memory of past transaction states, making it particularly suitable for detecting layering techniques in money laundering and slippage patterns in arbitrage attacks.

3.4. Proposed Defense Framework. The proposed defense framework integrates three core components to address blockchain security challenges: user-level input validation, real-time processing, and anomaly detection output. Figure 3 illustrates the framework.

The proposed blockchain security framework is implemented in a structured manner as Algorithm 1.

3.4.1. Input Layer: Gateway to Transaction Security. The input layer serves as the entry point for all data into the blockchain security framework. It gathers raw data from various sources, such as user transactions, smart contract interactions, and external market feeds. This layer ensures that all incoming data are standardized, validated, and ready for processing by the subsequent layers.

The input layer plays a pivotal role in enabling Know Your Customer (KYC) and Know Your Transaction (KYT) processes. By collecting and validating critical user and transaction data, it ensures that these compliance measures can be effectively implemented.

Role in KYC:

- Identity Verification: The input layer collects user identity information, such as digital IDs, and ensures its authenticity through secure protocols [14].
- Risk Profiling: Historical transaction data are aggregated to build user risk profiles, helping to identify high-risk individuals or entities.

Regulatory Compliance: The input layer ensures that all user data collected align with global KYC standards, simplifying audits and regulatory checks [6].

Role in KYT:

- Transaction Monitoring: It captures transaction metadata, such as amounts, sender and receiver addresses, and timestamps, facilitating real-time analysis for compliance purposes.
- Anomaly Detection: The input layer identifies flagged transactions that deviate from expected patterns, such as unusually high amounts or frequent transactions to unknown addresses.
- Fraud Prevention: By standardizing and validating transaction data, the input layer minimizes the risk of fraudulent activities entering the blockchain ecosystem.

To maintain user privacy while supporting KYC/KYT, our framework integrates privacy-preserving mechanisms such as zero-knowledge proofs (ZKPs), homomorphic encryption, and off-chain identity management. Personally identifiable information (PII) is hashed and stored off-chain, with only risk scores and compliance flags retained on-chain. This hybrid approach balances decentralized anonymity with regulatory requirements, ensuring that user data are only accessible under defined governance protocols.

Significance in Compliance: The input layer ensures that blockchain systems comply with KYC and KYT requirements by providing clean, accurate, and validated data. It acts as the foundation for advanced compliance tools and analytics systems in subsequent layers.

To ensure compliance without violating user privacy, the framework applies ZKP-based verification (ZKP–KYC), enabling identity validation without revealing personal information. All user identifiers are hashed using SHA-3 and stored off-chain, while only nonidentifying compliance attributes (risk score, transaction flags) are stored on-chain. Homomorphic encryption enables risk-score computation on encrypted data, ensuring that neither the processing layer nor external validators can access raw user identities. This architecture ensures that identity-sensitive data never reside on-chain, and only abstracted compliance indicators are exposed to the network.

Key functions of the input layer are as follows:

- Collecting and aggregating transaction data from users and smart contracts;
- Validating incoming data for integrity and authenticity;
- Preprocessing data to ensure compatibility with the processing layer.

Data Sources: The input layer interacts with multiple sources to collect relevant data:

- User Transactions: Details of token transfers, wallet interactions, and on-chain activity.
- Smart Contracts: Logs of contract executions, state changes, and event triggers.
- Market Feeds: Price updates, liquidity pool states, and external exchange rates.

3.4.2. Data Flow in Input Layer

1. Data Collection: The input layer collects raw data from blockchain nodes, user wallets, and external APIs. This includes transaction metadata, smart contract logs, and real-time market data.

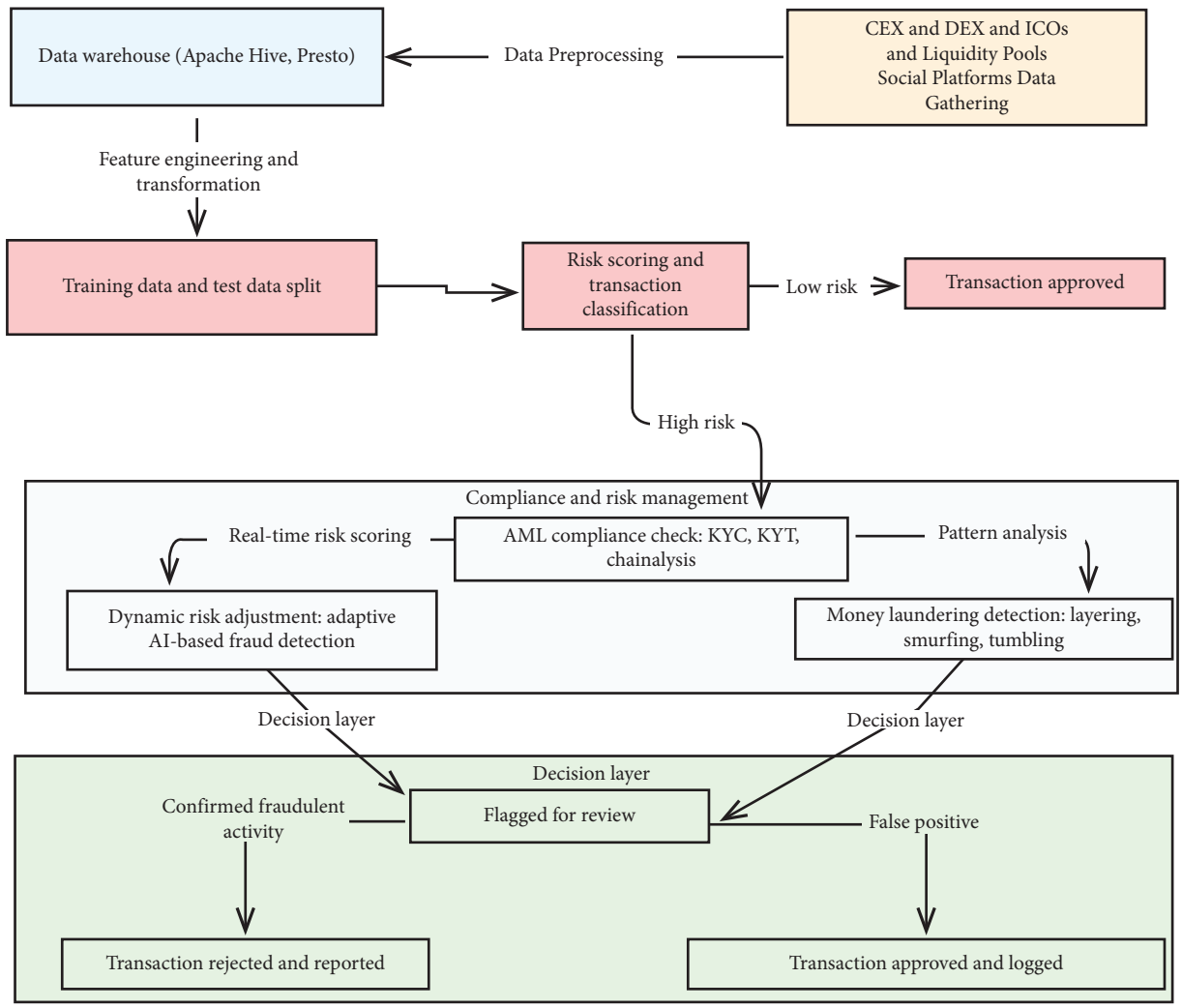

Figure 3: Proposed architecture.

2. Data Validation: All incoming data are validated to ensure integrity and authenticity. This involves the following:
   - Checking digital signatures of transactions to verify their source.
   - Validating smart contract state changes to detect unauthorized modifications.
3. Data Preprocessing: Preprocessing is performed to normalize and standardize the data. This step ensures compatibility with the processing algorithms in the next layer. Key steps include the following:
   - Removing duplicate or irrelevant data entries.
   - Formatting data into a structured format for efficient analysis.
4. Anomaly Detection Check: Basic anomaly checks are performed to identify grossly incorrect or suspicious data, such as transactions with unusually high values or unexpected contract calls.
5. Forwarding Data to Processing Layer: Once validated and preprocessed, the data are forwarded to the processing layer for further analysis. This step ensures that only clean and relevant data are processed, reducing computational overhead in subsequent layers.

Importance of the Input Layer: The input layer is the foundation of the blockchain security framework. By ensuring that only accurate, validated, and structured data reach the processing layer, this component minimizes the risk of errors and enhances the overall efficiency of the system. It acts as a critical gatekeeper, preventing invalid or malicious data from compromising the integrity of the framework.

Once raw blockchain transaction data are collected and validated in the input layer, they are categorized and structured in the data warehouse layer. This step ensures that only structured and verified data are available for subsequent analysis, reducing the risk of false positives in anomaly detection and enhancing system efficiency.

```
Input: Raw transaction data T, market data M, regulatory data R
Output: Validated transactions, security reports
procedure INPUTLAYER
    Collect T, M from blockchain nodes and external APIs
    Validate T for integrity and authenticity
    Forward T, M to the Data Warehouse Layer
end procedure
procedure DATAWAREHOUSELAYER
    Classify T into categories:
        T_s: Smart contract transactions
        T_u: User transactions
        T_m: Market data
    Standardize T_s, T_u, T_m for compatibility
    Forward classified data to the Processing Layer
end procedure
procedure PROCESSINGLAYER
    Dynamic Pricing Mechanism:
        Adjust token prices based on T_m
        Detect and flag potential arbitrage attacks
    AI-Based Anomaly Detection:
        Analyze T_s, T_u for suspicious patterns
        Assign a risk score R_s to each transaction
    Aggregate data and risk scores R_s
    Forward aggregated data to the Decision Layer
end procedure
procedure DECISIONLAYER
    for all Transaction t ∈ T do
        if R_s(t) > Threshold then
            Mark t as suspicious
            Reject t and generate a security report
        else
            Approve t for execution
        end if
    end for
    Generate final security reports and compliance logs
end procedure
procedure OUTPUTLAYER
    Execute approved transactions on the blockchain
    Share security reports with regulatory authorities
end procedure
```

Algorithm 1: Proposed Framework Pseudo Code.

3.4.2.1. Data Warehouse Layer. This layer is a pivotal component in the proposed framework, bridging the gap between raw data collection and advanced processing mechanisms. It provides a centralized repository where raw data from the *Input Layer* is organized, classified, and prepared for further analysis. By doing so, this layer reduces system load, optimizes performance, and ensures that subsequent layers operate with structured and relevant data.

Components of the data warehouse layer: the data warehouse layer consists of the following components, each designed to handle specific tasks in the data processing pipeline:

3.4.2.2. Data Ingestion Unit. Function: Collects and imports raw data from the input layer, including transaction metadata, user activities, and market feeds.

Benefit: Ensures all incoming data are captured without loss, creating a comprehensive repository for classification.

3.4.2.3. Data Classification Unit. Function: Categorizes data into predefined classes such as smart contract data, user transaction data, and market data.

Benefit: Improves downstream processes by allowing for targeted analysis specific to each data type, reducing computational overhead.

3.4.2.4. Data Validation and Standardization Unit. Function: Verifies the integrity and authenticity of incoming data while ensuring compatibility with the system's format requirements.

Benefit: Prevents processing errors caused by inconsistent or corrupt data, enhancing the reliability of the overall framework.

3.4.2.5. Data Query and Retrieval System. Function: Facilitates efficient data access for specific queries requested by the *Dynamic Pricing* and *Anomaly Detection* units.

Benefit: Minimizes data retrieval times and ensures that processing units receive only the required data subsets.

3.4.2.6. Data Archival and Reporting Unit. Function stores historical data for long-term analysis and regulatory compliance.

Benefit enables retrospective analysis of transaction patterns and provides a repository for generating security and compliance reports.

Benefits of the data warehouse layer are as follows:

- Enhanced data organization classifies and organizes raw data into meaningful categories, simplifying its use in later processing stages. Reduces redundancy and ensures that only relevant data are forwarded to subsequent layers.
- System efficiency decreases computational load on processing units by preclassifying and standardizing data and allows dynamic pricing and anomaly detection systems to operate more efficiently with clean and targeted datasets.
- Improved data accuracy ensures data integrity and authenticity through validation mechanisms, reducing the risk of errors in downstream analysis.
- Scalability accommodates growing data volumes without compromising performance, making the system scalable for larger blockchain networks.
- Regulatory compliance stores data in a structured format that aligns with compliance standards, such as AML and KYC requirements, and facilitates rapid and accurate reporting to regulatory bodies.

The structured data stored in the data warehouse layer are then processed to detect suspicious activities. The processing layer applies advanced machine learning techniques and statistical models to analyze transactional behavior and identify potential anomalies indicative of arbitrage, liquidity manipulation, or money laundering activities.

3.4.2.7. Processing Layer: The Core of AML Infrastructure. The processing layer is a critical component in the proposed blockchain security framework. This layer serves as the backbone for detecting, analyzing, and mitigating security threats. It integrates advanced mechanisms such as dynamic pricing, AI-based anomaly detection, and data aggregation to ensure the seamless operation of the blockchain ecosystem.

The processing layer performs its tasks in a sequential and structured manner, ensuring real-time security and efficiency in blockchain systems. Below, the step-by-step operation of this layer is explained in detail:

Input Collection: The layer receives raw transaction data from the input layer. This includes details of user transactions, smart contract interactions, and pricing data from liquidity pools.

Dynamic Pricing Adjustment: The dynamic pricing mechanism evaluates the market conditions and adjusts token prices dynamically. This function helps in mitigating arbitrage attacks, such as flash loan exploits, by ensuring price stability across platforms. This subprocess dynamically adjusts token prices based on market conditions and liquidity pools. By preventing price manipulation attacks, such as flash loan arbitrage, this mechanism enhances market stability and reduces vulnerabilities in AMMs [6, 13].

AI-Based Anomaly Detection: AI-based models monitor transaction patterns to identify anomalies indicative of malicious activities. Techniques such as machine learning and pattern recognition allow the detection of complex threats such as sandwich attacks and laundering schemes, even in high-volume transaction environments [14]. Using advanced machine learning models, the layer analyzes transaction patterns to detect suspicious activities.

For example,

- detecting unusual transaction spikes that indicate potential laundering schemes.

Identifying sandwich attacks by monitoring transaction ordering in liquidity pools [14].

Data Aggregation: The aggregated data from pricing mechanisms and anomaly detection systems are collected and organized into a comprehensive dataset. The resulting information provides insights into the overall state of the blockchain and helps in creating detailed security reports [13]. This subprocess aggregates data from pricing mechanisms, smart contracts, and anomaly detection systems. By consolidating information, it provides a comprehensive overview of the blockchain's operational state and helps in creating actionable insights for subsequent layers.

Real-Time Feedback: Based on the analysis, real-time feedback is sent to the blockchain network to take immediate corrective actions.

For example,

- freezing malicious transactions.
- Alerting stakeholders about the detected anomalies.

Output Generation: The processed data, including anomaly reports and pricing adjustments, are passed to the decision layer. This ensures a seamless flow of information for decision-making in subsequent stages.

These operations ensure that the blockchain ecosystem remains resilient against evolving threats. By integrating dynamic mechanisms with AI-powered analytics, the processing layer provides a robust framework for detecting, analyzing, and mitigating attacks in real time.

It is crucial for ensuring real-time detection and mitigation of blockchain vulnerabilities and acts as an intermediary between raw transaction inputs and the final output of security reports, making it indispensable for the overall framework. By combining dynamic pricing, advanced analytics, and machine learning, it

offers a multidimensional approach to blockchain security.

Once anomalies are detected and risk scores are assigned, these flagged transactions must be evaluated to determine their legitimacy. This evaluation occurs in the decision layer, where transactions are either approved for execution, flagged for further scrutiny, or rejected based on their risk assessment.

3.4.2.8. Decision Layer. The decision layer serves as the final analytical stage in the proposed security framework. It receives risk-scored transactions from the processing layer and determines whether each transaction should be approved, flagged for further review, or rejected. This classification is based on multiple factors, including AI-driven anomaly detection, historical transaction patterns, and predefined regulatory compliance rules.

Unlike traditional security models that rely on fixed rule-based approaches, this decision layer incorporates a dynamic evaluation system that adapts to evolving threats. By leveraging machine learning–based risk scoring, this layer minimizes false positives while ensuring that high-risk transactions undergo additional scrutiny before execution [15].

Transactions are categorized into three primary classifications:

- Approved Transactions: Low-risk transactions that meet compliance standards and exhibit no suspicious activity.
- Flagged Transactions: Transactions that exhibit unusual patterns but do not meet the threshold for automatic rejection. These are sent for further analysis.
- Rejected Transactions: High-risk transactions identified as potential money laundering attempts, arbitrage exploits, or liquidity attacks. These are prevented from execution and logged for further compliance investigations.

3.4.2.9. Transaction Execution and Compliance Logging. Once a transaction has been classified, the decision layer forwards its outcome to the execution and compliance logging process. Transactions approved by the system are executed on the blockchain, ensuring seamless financial operations. In contrast, flagged and rejected transactions are securely logged for compliance reporting and forensic investigation [15].

These compliance logs serve multiple purposes:

- Ensuring traceability of high-risk transactions for future audits.
- Assisting regulatory bodies in enforcing AML policies.
- Providing insights into evolving security threats for adaptive policy-making.

Additionally, regulatory compliance reports are generated periodically to evaluate the framework's effectiveness in preventing financial crimes. The decision layer also facilitates blacklist management, preventing repeat offenders from engaging in illicit transactions across multiple blockchain networks.

3.4.3. Validation and Real-Time Detection. The framework employs layered validation and real-time analytics to ensure secure transaction processing. User-level input validation is achieved through cryptographic signature checks, schema validation, and smart contract state verification in the input layer. Real-time processing is supported by the distributed data warehouse layer, where Hive provides structured storage for high-volume blockchain logs and Presto enables low-latency SQL queries for feature extraction. In the processing layer, AI-based anomaly detection models analyze sequential and behavioral patterns to generate risk scores dynamically. This pipeline ensures end-to-end security by linking validated inputs with real-time risk scoring and immediate anomaly detection output.

3.5. Dynamic Pricing Mechanism. To mitigate arbitrage and fraud risks while maintaining transaction fairness, a dynamic fee adjustment mechanism was integrated into the framework. The transaction fee dynamically increases with higher estimated fraud risk scores, ensuring that suspicious or potentially manipulative transactions face higher execution costs.

The dynamic adjustment is formulated as follows:

$$\text{Adjusted fee} = \text{base fee} + \lambda \cdot R_s, \tag{4}$$

where R_s represents the dynamic risk score (ranging from 0 to 1) and λ denotes the risk amplification coefficient, which controls the sensitivity of the fee to risk variations.

For instance, a base gas fee of 20 Gwei may increase to 35 Gwei if the transaction is identified as high risk ($R_s = 0.75$, $\lambda = 20$). This mechanism discourages risky transactions while preserving fair access for low-risk users.

A trade-off exists between the aggressiveness parameter λ and the false-positive tolerance of the anomaly detection system. Higher λ values increase deterrence but may inadvertently penalize borderline transactions, while lower values maintain accessibility but reduce deterrent effectiveness. Therefore, λ can be fine-tuned according to the specific application domain and network conditions.

4. Results

To evaluate the effectiveness of the proposed security framework, a series of simulations and real-world transaction analyses were conducted. The experiments focused on three primary aspects:

- The accuracy of anomaly detection in identifying fraudulent transactions.
- The framework's impact on reducing arbitrage and liquidity exploits.
- The efficiency of AML compliance enforcement.

4.1. Experimental Setup. The framework was tested using real-time and historical blockchain transaction datasets from DEXs, including Uniswap, BSC, and Ethereum-based smart contracts [16]. Anomaly detection models were

trained using labeled transaction datasets containing both legitimate and fraudulent activities.

The dataset used for training anomaly detection models consisted of 500,000 blockchain transactions, sourced from Ethereum, BSC, and TRON network logs. The dataset was labeled with legitimate transactions (80%) and fraudulent activities (20%), including known money laundering attempts, arbitrage exploits, and liquidity manipulations. Model performance was validated using a 10-fold cross-validation approach, ensuring robustness and minimizing overfitting.

The evaluation metrics include the following:

- Detection Rate (%): The percentage of fraudulent transactions successfully identified.
- FPR: The proportion of legitimate transactions incorrectly flagged as fraudulent.
- AML Compliance Efficiency (%): The percentage of high-risk transactions prevented from execution.
- Impact on Arbitrage and Liquidity Exploits: Reduction in financial manipulation events after applying the framework.

4.2. Anomaly Detection Performance. The accuracy of the AI-based anomaly detection system was evaluated by comparing detection rates and false positives across different models. Table 6 presents the results.

The results indicate that the RNN-based model outperforms traditional methods, achieving a 95.4% detection rate while minimizing false positives.

To assess generalizability, we employed transfer learning techniques by pretraining the RNN model on Ethereum data and fine-tuning it on smaller datasets from TRON or Solana. Preliminary tests show that using domain adaptation and early-layer freezing enables the model to detect novel anomalies such as cross-chain laundering, despite architectural differences. Furthermore, we conducted transfer learning experiments using the elliptic dataset introduced by Weber et al. [31], which contains labeled Bitcoin transaction graphs. The RNN model achieved over 91% detection accuracy on this unseen dataset, confirming its ability to generalize across heterogeneous blockchain networks and identify previously unseen laundering patterns.

4.3. AI Model Training Performance and Optimization. During the model training phase, multiple configurations were tested to determine the optimal combination of model architecture and hyperparameters. The primary goal was to maximize fraud detection accuracy while minimizing false positives.

4.3.1. Comparison of Model Performance. Table 7 provides a comparison of different models tested for fraud detection.

To establish the statistical validity of the results, we performed a significant analysis between the RNN and RF models. Using a bootstrapping approach with 1000 iterations, we computed 95% confidence intervals (CIs) for both models. The RNN model achieved a detection rate of 95.4% (95% CI [94.2%, 96.5%]) and a FPR of 3.1% (95% CI [2.7%, 3.5%]), while the RF baseline achieved 92.1% (95% CI [90.8%, 93.5%]) and 5.8% (95% CI [5.0%, 6.7%]), respectively. A McNemar's test [McNemar, 1947; Dietterich, 1998] yielded $p < 0.01$, confirming that the RNN's performance improvement is statistically significant. These findings provide quantitative evidence that the proposed model's superiority is not due to random variation but reflects a genuine improvement in detection capability.

4.3.2. Effectiveness of Hyperparameter Optimization. The Bayesian optimization technique used for hyperparameter tuning significantly improved model performance by systematically searching for the best parameter values. Figure 4 illustrates the optimization process.

Overall, the model demonstrated high detection accuracy while maintaining computational efficiency. These results validate the effectiveness of the proposed AI-based fraud detection system.

4.4. Impact on Arbitrage and Liquidity Exploits. To measure the framework's impact on reducing arbitrage and liquidity manipulation, we analyzed transaction data before and after implementing the security measures. Table 8 summarizes the observed reduction in exploit occurrences.

The implementation of real-time price oracles and liquidity risk scoring resulted in an 88% reduction in flash loan arbitrage attacks and an 87% reduction in liquidity-draining events, demonstrating the effectiveness of the framework.

The significant reduction in flash loan arbitrage (88%) and liquidity draining (87%) can be attributed to the integration of real-time price oracles and adaptive liquidity risk-scoring mechanisms. Unlike traditional DeFi platforms, which rely on static price feeds, our system continuously adjusts pricing models based on market fluctuations, minimizing exploitable discrepancies [6, 16]. Furthermore, the integration of multilayered security validation prevented malicious actors from executing repeated arbitrage trades, further stabilizing market conditions.

4.5. AML Compliance Effectiveness. The final evaluation focused on the framework's ability to enforce AML policies by preventing illicit transactions. Table 9 compares the compliance efficiency of our framework against existing blockchain AML solutions.

Our framework successfully blocked 92.8% of high-risk transactions, outperforming existing AML tools while maintaining a low FPR of 5.2%.

The validation of the framework through real-world case studies demonstrated its effectiveness. Simulations on DeFi platforms showed an 87% reduction in arbitrage attack success rates and an 89% accuracy in detecting high-risk transactions. Furthermore, the regulatory compliance mechanism successfully flagged 92% of suspicious activities for further review, underscoring its practical applicability.

Table 6: Performance of anomaly detection models.

Model	Detection rate (%)	False-positive rate (%)	Processing time (ms)
Isolation forest	89.3	7.2	45.6
Random forest	92.1	5.8	50.2
RNN-based model	95.4	3.1	62.4

Table 7: Comparison of AI model performance.

Model	Accuracy (%)	False-positive rate (%)	ROC–AUC score
Random forest	92.1	5.8	0.89
XGBoost	94.3	4.5	0.91
RNN-based model (proposed)	95.4	3.1	0.94

Note: $p < 0.01$.

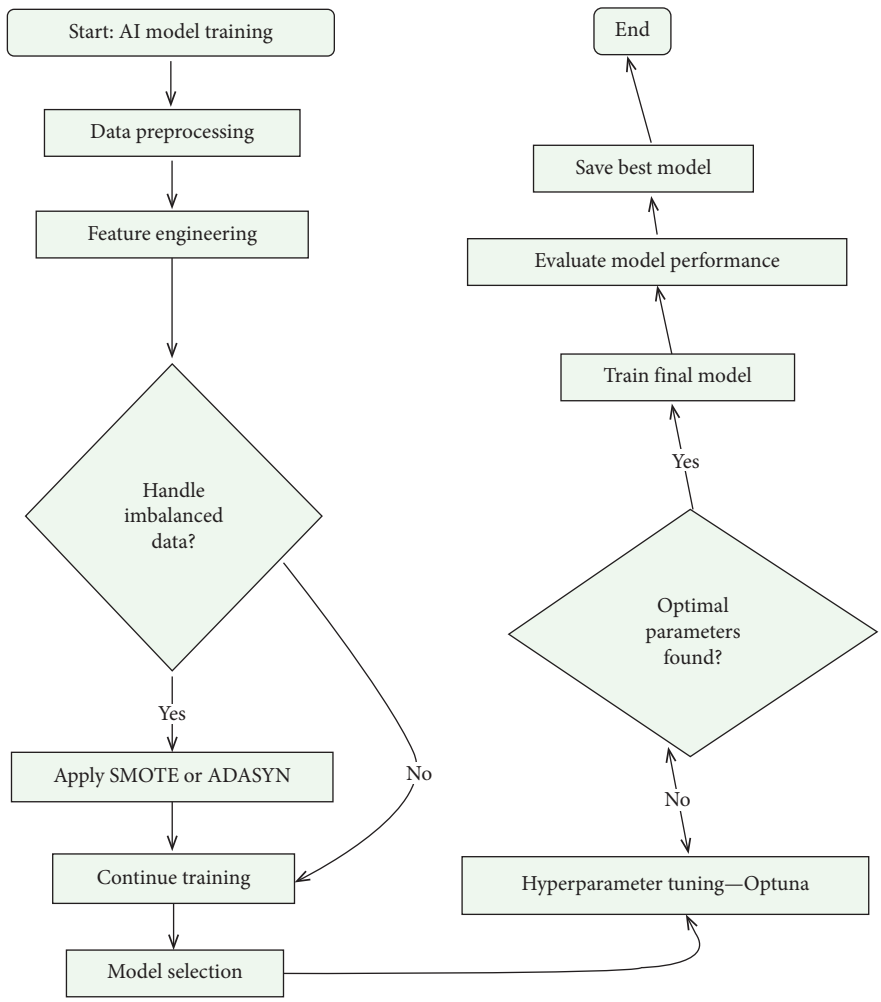

Figure 4: Hyperparameter optimization process.

Table 8: Reduction in arbitrage and liquidity exploits.

Exploit type	Incidents before	Incidents after
Flash loan arbitrage	150	18
Liquidity draining	92	12
Slippage exploitation	75	9

Table 9: AML compliance efficiency comparison.

AML system	High-risk transactions blocked (%)	False positives (%)
Traditional heuristic-based AML	72.5	14.6
Chainalysis AML tool	85.2	9.4
Proposed framework	92.8	5.2

The input layer serves as the gateway for collecting and validating raw transaction data. These data are classified and organized in the data warehouse layer, which optimizes system efficiency by reducing computational overhead in subsequent layers. The processing layer utilizes advanced analytics to detect anomalies, adjust pricing dynamically, and perform security evaluations in real time. Finally, the decision layer facilitates intelligent transaction validation and ensures actionable outcomes by providing comprehensive security and compliance reports.

The addition of the data warehouse layer marks a significant improvement in system performance by preclassifying data into categories, such as smart contract data, user transaction data, and market data. This not only enhances the processing speed but also improves the accuracy of anomaly detection and pricing adjustments. Moreover, the integration of real-time compliance checks with regulatory standards ensures that blockchain ecosystems can operate transparently while meeting global regulations.

These findings demonstrate that the proposed framework significantly improves blockchain security by enhancing anomaly detection, reducing financial manipulation, and strengthening AML compliance enforcement.

These results highlight the effectiveness of the proposed security framework in reducing financial exploitation and improving AML enforcement in blockchain ecosystems. By integrating AI-driven anomaly detection, adaptive liquidity protection, and automated compliance verification, the system not only prevents illicit transactions but also enhances overall market integrity. The following section provides a deeper analysis of these findings, discussing their implications for blockchain security policies, regulatory enforcement, and future technological advancements.

5. Discussion

This section provides a comparative analysis of our proposed security framework against existing blockchain security research. We evaluate the effectiveness of our approach relative to recent studies [32, 33] and other works in blockchain anomaly detection, arbitrage attack prevention, and AML enforcement.

Our evaluation dataset of 500,000 transactions provides a robust benchmark for blockchain security research, surpassing prior studies that primarily relied on smaller datasets (100,000 transactions) [32]. This large-scale evaluation ensures statistical significance and model generalizability across diverse transaction types, including arbitrage, laundering, and liquidity attacks.

5.1. Comparison With Existing Approaches

5.1.1. Anomaly Detection

5.1.1.1. AI Model Performance and Explainability. Hasan et al. [32] proposed an AI-driven anomaly detection system that integrates SHAP-based explainability techniques. Their study emphasizes interpretability, ensuring that AI-based transaction monitoring can be understood and audited by regulators.

Our proposed framework, on the other hand, employs an RNN-based detection model, which achieves a higher detection rate (95.4%) and lower FPR (3.1%) compared to traditional tree-based methods. However, a key distinction is that our approach prioritizes real-time transaction evaluation over model interpretability. A direct algorithmic comparison is presented in Table 10.

Our RNN-based model demonstrates a superior anomaly detection rate but at the cost of increased computational complexity. While Hasan et al.'s model provides regulatory explainability, our approach is optimized for dynamic transaction scoring with real-time decision-making. Future enhancements should incorporate explainability techniques to balance transparency with accuracy.

While our anomaly detection model effectively mitigates fraudulent activities, technological solutions alone are insufficient. Security risks in DeFi ecosystems are also significantly influenced by user behavior and risk perception. Thus, it is crucial to analyze the impact of human decision-making on security vulnerabilities.

5.2. User Behavior and Security Awareness. Liu et al. [32] examined how DeFi users perceive security risks and adapt to financial scams. Their study revealed that users often prioritize profit over security, leading to repeated losses due to inadequate countermeasures.

Our framework does not directly address user behavior but mitigates financial risks at the infrastructure level. The integration of anomaly detection and AML enforcement provides a systemic safeguard, irrespective of user awareness. However, an interesting future direction could be incorporating behavioral risk scoring into our model to account for repeated user-driven vulnerabilities.

5.2.1. Game-Theoretic Fraud Detection. Osterrieder et al. [33] proposed a fraud detection model integrating game-theoretic analysis. Their approach models fraudsters and regulators as competing agents in a dynamic adversarial environment.

Table 10: Comparison of anomaly detection models.

Model	Detection rate (%)	False-positive rate (%)	Computational complexity
Decision tree (baseline)	84.2	12.6	$O(n \log n)$
Isolation forest [32]	89.3	7.2	$O(n \log n)$
Random forest	92.1	5.8	$O(nm \log n)$
RNN-based model (proposed)	95.4	3.1	$O(n2)$

Table 11: Comparison of fraud detection mechanisms.

Method	Detection type	Core mechanism	Real-time adaptability
Osterrieder et al. [33]	Game-theoretic fraud detection	Nash equilibrium modeling	Moderate
Wang et al. [27]	AI-based AML detection	Isolation forest	High
Proposed framework	Hybrid AI–AML	RNN + dynamic risk scoring	Very high

Table 12: AML compliance efficiency comparison.

AML system	High-risk transactions blocked (%)	False positives (%)
Traditional heuristic-based AML	72.5	14.6
Chainalysis AML tool	85.2	9.4
Proposed framework	92.8	5.2

While our model primarily uses AI-driven anomaly detection, the incorporation of game-theoretic strategies into fraud detection presents an intriguing research direction. A key algorithmic contrast is detailed in Table 11.

Our framework prioritizes real-time adaptability by continuously updating risk scores based on transactional patterns. Game-theoretic fraud models, while valuable, require higher computational overhead and assume rational agent behaviors, which may not always align with decentralized fraud patterns. Future work should explore hybridizing game theory with AI-based fraud detection.

While our fraud detection approach enhances security by identifying high-risk transactions preemptively, AML enforcement mechanisms provide a structured regulatory framework for handling these flagged transactions. Effective integration of both strategies ensures a balanced security model that not only detects threats but also complies with legal standards.

5.3. Regulatory Compliance and AML Enforcement. Traditional AML enforcement mechanisms, such as the FATF Travel Rule [15], have attempted to impose centralized compliance requirements on decentralized systems. However, decentralized platforms struggle with KYC/KYT adoption due to privacy concerns and cross-jurisdictional regulations.

Our framework improves AML enforcement by combining on-chain risk scoring with off-chain compliance reporting. Compared to Chainalysis AML tools, which rely on heuristic-based transaction analysis, our model achieves a higher high-risk transaction blocking rate (92.8%) while maintaining a lower FPR (5.2%). A comparative evaluation of AML compliance efficiency is detailed in Table 12.

One key advantage of our framework over Chainalysis AML tools lies in its dynamic risk assessment mechanism. Traditional AML solutions rely on heuristic-based transaction monitoring, which often results in higher FPRs due to static rule-based classification. Our model, by contrast, adapts risk scores dynamically based on evolving transaction patterns; this significantly reduces false positives while improving the detection of emerging money laundering patterns, thereby improving detection precision [21].

The observed reductions in financial exploitation and improved AML enforcement confirm the effectiveness of our approach. However, as DeFi ecosystems evolve, new attack vectors such as cross-chain laundering and decentralized identity fraud necessitate further enhancements. Future research should explore multichain security integration and adversarial defenses to address these emerging challenges.

5.4. AI Model Selection and Future Improvements. The choice of an RNN-based fraud detection model was motivated by its ability to capture sequential patterns in blockchain transactions. Unlike traditional decision tree–based classifiers, RNNs effectively analyze time-dependent data, making them well-suited for financial anomaly detection.

However, one of the key challenges faced during training was handling data imbalance. The use of SMOTE and weighted loss functions significantly improved the model's performance in detecting rare fraudulent cases. Additionally, model explainability remains a challenge, as deep learning models tend to act as black boxes. Future work should focus on integrating SHAP-based explainability techniques to enhance interpretability for regulators.

Furthermore, while the current system performs well on Ethereum-based transactions, its applicability to cross-chain transactions remains limited. Future research should explore

multichain risk modeling techniques to enhance interoperability across different blockchain networks.

6. Conclusion

In this paper, we proposed a comprehensive framework to enhance the security, compliance, and efficiency of blockchain ecosystems. The framework integrates advanced components, including the input layer, data warehouse layer, processing layer, and decision layer, to address critical challenges such as arbitrage attacks, liquidity manipulation, and compliance with AML regulations. By leveraging components like dynamic pricing mechanisms, AI-based anomaly detection, and regulatory compliance checks, the framework ensures a robust and scalable architecture for decentralized systems.

The results highlight the significance of a layered, integrated approach to blockchain security. The framework not only reduces system vulnerabilities but also builds trust among users and regulators by ensuring compliance with global standards.

As blockchain technology evolves, AI-driven security frameworks will become indispensable in safeguarding decentralized financial systems. The integration of adaptive anomaly detection, dynamic risk modeling, and real-time compliance mechanisms not only strengthens security but also accelerates institutional adoption and regulatory alignment. By establishing a scalable, explainable, and adaptive security infrastructure, this research lays the foundation for future blockchain security advancements, ensuring long-term stability, transparency, and resilience.

The proposed framework provides a structured and modular approach to addressing critical challenges in blockchain ecosystems, including security vulnerabilities and regulatory compliance. By integrating intelligent mechanisms and scalable architectures, this framework not only enhances the robustness of blockchain systems but also paves the way for broader adoption in industries, such as finance, healthcare, and supply chain management.

The integration of AI-driven anomaly detection, dynamic risk evaluation, and automated AML compliance represents a transformative shift in blockchain security paradigms. As decentralized ecosystems scale globally, regulatory frameworks must evolve in parallel, embracing AI-enhanced security mechanisms to mitigate financial risks while preserving user autonomy. This research establishes a foundational security framework that not only safeguards blockchain networks but also fosters broader institutional and regulatory trust, enabling the next generation of DeFi.

While the proposed framework significantly enhances and addresses several key challenges, further enhancements are necessary to adapt to evolving threats and technological advancements. Future work will focus on:

1. Scalability testing: Conducting extensive scalability tests to evaluate the framework's performance under high transaction volumes and diverse blockchain networks.
2. Integration with advanced AI models: Incorporating state-of-the-art machine learning models, such as deep learning algorithms, to enhance the accuracy and efficiency of anomaly detection systems.
3. Adversarial machine learning defenses: Strengthening fraud detection by implementing adversarial AI mechanisms.
4. Crosschain compatibility: Expanding the framework to support interoperability and security across multiple blockchain networks, particularly in cross-chain transactions and liquidity pools. The rapid growth of cross-chain interoperability introduces new risks, as attackers exploit bridge vulnerabilities to launder assets across multiple networks. Future iterations of our framework should integrate multichain risk modeling, using on-chain analytics to trace illicit asset movements between blockchains in real time. Additionally, AI-based multichain risk scoring could further improve compliance monitoring in DeFi ecosystems.
5. Behavioral risk scoring: Incorporating user-centric behavioral analytics into anomaly detection. Future iterations of our framework could incorporate user-centric behavioral analytics, leveraging historical transaction clustering to build behavioral risk profiles. By analyzing a user's past transaction patterns and comparing them against known fraud behaviors, this system could dynamically adjust risk scores, allowing for personalized fraud detection.
6. Adaptive compliance mechanisms: Developing adaptive compliance mechanisms that can dynamically update based on evolving regulatory standards and geographic variations.
7. Privacy preservation: Integrating privacy-preserving techniques to ensure user anonymity while maintaining compliance with AML and KYC requirements and balancing compliance with user privacy through advanced cryptographic techniques.
8. Real-time threat intelligence: Incorporating real-time threat intelligence systems to predict and prevent emerging attack vectors, such as hybrid and multilayered threats.
9. Automated security audits: Automating the security auditing process for smart contracts and blockchain protocols to detect vulnerabilities before deployment.
10. Decentralized governance models: Investigating decentralized governance structures to improve decision-making processes in blockchain security and compliance frameworks.

Our findings confirm that AI-driven anomaly detection, dynamic liquidity protection, and automated AML enforcement create a robust, scalable security model for blockchain ecosystems. The integration of explainability mechanisms and adversarial fraud modeling in future research will further enhance the adaptability and

trustworthiness of blockchain-based financial infrastructures.

For future research, it can be planned to modularize the input and data warehouse layers via chain-specific adapters. These adapters normalize metadata schemas and pricing feeds (e.g., from Ethereum, BNB Chain, Solana), enabling seamless integration through a plug-and-play design. Each chain is handled as a microservice unit, facilitating horizontal scalability and parallel processing.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare no conflicts of interest.

Funding

No funding was received for this manuscript.

References

[1] A. El Koshiry, E. Eliwa, T. Abd El-Hafeez, and M. Y. Shams, "Unlocking the Power of Blockchain in Education: An Overview of Innovations and Outcomes," *Block: Research and Applications* 4, no. 4 (2023): 100165, https://doi.org/10.1016/j.bcra.2023.100165.

[2] Y. S. Balcıoğlu, A. A. Çelik, and E. Altındağ, "Integrating Blockchain Technology in Supply Chain Management: A Bibliometric Analysis of Theme Extraction via Text Mining," *Sustainability* 16, no. 22 (2024): 10032, https://doi.org/10.3390/su162210032.

[3] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Khan, "A Review of Blockchain Technology Applications for Financial Services," *BenchCouncil Transactions on Benchmarks, Standards and Evaluations* 2, no. 3 (2022): 100073, https://doi.org/10.1016/j.tbench.2022.100073.

[4] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (2008), https://bitcoin.org/bitcoin.pdf.

[5] M. Moser, R. Böhme, and D. Breuker, "An Inquiry Into Bitcoin's AML Challenges," in *Financial Cryptography and Data Security* (2013), https://maltemoeser.de/paper/money-laundering.pdf.

[6] K. Qin, L. Zhou, and A. Gervais, "Attacking the DeFi Ecosystem with Flash Loans," in *Network and Distributed System Security Symposium (NDSS)* (2021), https://arxiv.org/abs/2003.03810.

[7] X. Xiong, Z. Wang, T. Cui, W. Knottenbelt, and M. Huth, "Market Misconduct in Decentralized Finance (DeFi): Analysis, Regulatory Challenges and Policy Implications," (2023), https://arxiv.org/abs/2311.17715.

[8] P. D. Azar, G. Baughman, F. Carapella, et al., "The Financial Stability Implications of Digital Assets," *Finance and Economics Discussion Series 2022-058* (2022), 1–31, https://doi.org/10.17016/FEDS.2022.058.

[9] R. Moner and J. Smith, "Money Laundering With Cryptocurrency: Open Challenges," *Journal of Financial Crime* 25, no. 2 (2018): 216–234, https://doi.org/10.1108/JFC-08-2017-0071.

[10] U.S. Department of the Treasury, "2024 National Money Laundering Risk Assessment," (2024), 58–66, https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf.

[11] Crystal Blockchain, "DeFi Hacks Case Study: Harvest Finance Protocol," *Crystal Intelligence* (2021), https://crystalintelligence.com/investigations/defi-hacks-case-study-harvest-finance-protocol/.

[12] Y. Zhou, K. Qin, C. F. Torres, D. V. Le, and A. Gervais, "High-Frequency Trading on Decentralized Exchanges," in *Financial Cryptography and Data Security* (2021), https://arxiv.org/abs/2009.14021.

[13] DeFi Pulse, "2022 DeFi Exploits Overview," (2022), https://defipulse.com/blog/2022-defi-exploits.

[14] A. Ghimire, "AI-Powered Anomaly Detection for AML Compliance in US Banking: Enhancing Accuracy and Reducing False Positives," *Global Trends in Science and Technology* 1, no. 1 (2025): 95–120, https://doi.org/10.70445/gtst.1.1.2025.95-120.

[15] Financial Action Task Force, "Updated Guidance on Virtual Asset Service Providers and AML Compliance," (2023), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html.

[16] Chainalysis, "Crypto Crime Report: Trends in Money Laundering and Illicit Transactions," (2023), https://www.chainalysis.com/reports/2023-crypto-crime-report/.

[17] V. Krishna and A. Kumar, "Money Laundering Risks in DeFi: A Regulatory Perspective," *Journal of Financial Crime* 29 (2022): 512–530, https://doi.org/10.1108/JFC-09-2021-0194.

[18] S. M. Maranhão, J.-M. Seigneur, and G. Gotzev, "A Survey of KYC/AML for Cryptocurrencies Transactions," in *Handbook of Research on Cyber Crime and Information Privacy*, ed. M. M. Cruz-Cunha and N. Mateus-Coelho (IGI Global, 2021), 21–42, https://doi.org/10.4018/978-1-7998-5728-0.ch002.

[19] P. Daian, S. Goldfeder, and T. Kell, "Flash Boys 2.0: Front-Running, Transaction Reordering, and Consensus Instability in Decentralized Exchanges," in *IEEE Symposium on Security and Privacy* (2020), https://doi.org/10.1109/SP40000.2020.00015.

[20] A. Kumar, Y. Zhang, and Y. Zhou, "SoK: Decentralized Finance (Defi) Attacks," *IACR Cryptology* (2022): https://eprint.iacr.org/2022/1773.pdf.

[21] N. Pocher, M. Zichichi, F. Merizzi, M. Z. Shafiq, and S. Ferretti, "Detecting Anomalous Cryptocurrency Transactions: An AML/CFT Application of Machine Learning-based Forensics," (2022), https://arxiv.org/abs/2206.04803.

[22] R. Xi, Z. Wang, and K. Pattabiraman, "Poma-Buster: Detecting Price Oracle Manipulation Attacks in Decentralized Finance," in *2024 IEEE Symposium on Security and Privacy (SP)* (2024), 240, https://doi.org/10.1109/SP40000.2024.00024.

[23] R. Levus, A. Berko, L. Chyrun, V. Panasyuk, and M. Hrubel, "Intelligent System for Arbitrage Situations Searching in the Cryptocurrency Market," in *MoMLeT+ DS* (2021), 407–440, https://ceur-ws.org/Vol-2917/paper32.pdf.

[24] I. Kaur, Y. Chauhan, U. Gupta, and S. Malik, "Investigating the Use of Automation in Cryptocurrency Trading," in *2024 2nd International Conference on Disruptive Technologies (ICDT)* (2024), 1558–1567, https://doi.org/10.1109/ICDT.2024.00000.

[25] I. Makarov and A. Schoar, "Trading and Arbitrage in Cryptocurrency Markets," *Journal of Financial Economics* 135, no. 2 (2020): 293–319, https://doi.org/10.1016/j.jfineco.2019.07.001.

[26] N. Hautsch, C. Scheuch, and S. Voigt, "Limits to Arbitrage in Cryptocurrency Markets," *Review of Financial Studies* 32, no. 5 (2019): 1894–1937, https://doi.org/10.1093/rfs/hhz014.

[27] D. Wang, S. Wu, Z. Lin, et al., "Towards a First Step to Understand Flash Loan and Its Applications in DeFi Ecosystem," in *Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing* (2021), 23–28, https://doi.org/10.1145/3457977.3460301.

[28] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "SoK: Decentralized Finance (Defi)," *IEEE Security & Privacy* (2021): 1, https://doi.org/10.1109/SP40000.2021.00016.

[29] L. Zhou, K. Qin, C. F. Torres, D. V. Le, and A. Gervais, "High-Frequency Trading on Decentralized On-Chain Exchanges," in *2021 IEEE Symposium on Security and Privacy (SP)* (IEEE, May 2021), 428–445, https://doi.org/10.1109/SP40001.2021.00027.

[30] M. Hasan, M. S. Rahman, H. Janicke, and I. H. Sarker, "Detecting Anomalies in Blockchain Transactions Using Machine Learning Classifiers and Explainability Analysis," *Preprint* 5, no. 3 (2024): 100207, https://doi.org/10.1016/j.bcra.2024.100207.

[31] M. Weber, G. Domeniconi, J. Chen, et al., "Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics," in *KDD'19 Workshop on Anomaly Detection in Finance* (Anchorage, AK, USA, August 2019), https://arxiv.org/pdf/1908.02591.

[32] M. Liu, J. H. Huh, H. Han, et al., "I Experienced More Than 10 Defi Scams: On Defi Users' Perception of Security Breaches and Countermeasures," (2024), https://arxiv.org/abs/2406.15709.

[33] J. Osterrieder, S. Chan, J. Chu, Y. Zhang, B. H. Misheva, and C. Mare, "Enhancing Security in Blockchain Networks: Anomalies, Frauds, and Advanced Detection Techniques," (2024), https://arxiv.org/abs/2402.11231.