International Journal of Modern Computation, Information, and Communication Technology
2025;8(2):1-9.
ISSN: 2581-5954

On-Chain Transaction Anomaly Detection Using BlockSecAnalyzer for Blockchain Forensics

CH Nishanthi[1], Alexander Muthurengan Murugaiyan[2*], Tamilthaaragai Muthukumar[3]

[1]*Faculty of Science and Technology, Bournemouth University, Dorset, Bournemouth, UK.*
[2]*Department of Computing and Information Systems, University of Seychelles, Anse Royale, Seychelles.*
[2]*Chime Financial Inc, San Francisco, California, United States.*

[*]*Corresponding author: alexander.murugaiyan@unisey.ac.sc*

Abstract. Blockchain ecosystems require continuous surveillance to detect anomalous on-chain transactions and mitigate illicit activities such as fraud, money laundering, and unauthorized smart contract interactions. This study presents BlockSecAnalyzer, an analytical framework designed for on-chain transaction anomaly detection to support blockchain forensics. The proposed approach analyses transaction patterns to identify deviations from normal behaviour, including abnormal transaction volumes, rapid fund movements, and atypical smart contract interactions. BlockSecAnalyzer integrates machine learning techniques with statistical modelling to generate transaction-level alerts and actionable forensic insights. Real-time monitoring enables early identification of suspicious activities, while continuous analysis supports proactive threat mitigation strategies. Experimental evaluation demonstrates the effectiveness of the proposed framework in enhancing the security and resilience of blockchain networks against fraudulent and malicious operations.

Keywords: BlockSecAnalyzer, On-Chain Transaction Detection, Blockchain Forensics, Anomaly Detection, Threat Monitoring.

INTRODUCTION

Blockchain technology has transformed digital transactions by recording data decentralised, transparently, and immutably. Blockchain-based systems like Bitcoin, Ethereum, and others are growing more popular for cryptocurrencies, DeFi, and smart contracts, making security and integrity vital. Blockchain is secure by design, but its openness makes it vulnerable to fraud, money laundering, and other illegal acts. As blockchain technology grows, spotting suspicious or anomalous on-chain actions is crucial for asset protection and ecosystem confidence. This study examines how BlockSecAnalyzer, a sophisticated blockchain forensics tool, may discover on-chain transaction abnormalities for threat monitoring and analysis. BlockSecAnalyzer analyses blockchain transaction data in real time to discover unusual patterns that may signal malicious activity. BlockSecAnalyzer prevents fraud, security breaches, and other illicit actions by analysing transaction history and finding abnormalities such as unexpected transaction volumes, addresses, or frequency patterns. This paper shows how BlockSecAnalyzer can improve blockchain forensics and make blockchain environments safer and more trustworthy.

The expanding complexity and number of blockchain transactions make it harder to identify fraudulent, criminal, or suspicious activity manually. Blockchain networks create massive volumes of data and are decentralised, making traditional transaction monitoring techniques unsuitable. Detecting on-chain transaction abnormalities manually or with simple tools is time-consuming and error-prone, particularly as blockchain use rises. Malicious actors may use weaknesses to launder money, front-run, or steal cash without effective threat monitoring tools. BlockSecAnalyzer automates transaction data monitoring and analysis, enabling blockchain administrators to quickly find and address on-chain abnormalities. This study shows BlockSecAnalyzer can identify on-chain transaction abnormalities for blockchain forensics and threat monitoring. BlockSecAnalyzer monitors blockchain networks for suspicious activity using powerful machine learning, statistical analysis, and anomaly detection. Integrating BlockSecAnalyzer into blockchain security frameworks provides a complete solution to real-time risk identification and mitigation. BlockSecAnalyzer automatically analyses transaction data to identify risks and suggest additional study. BlockSecAnalyzer' s capacity to rapidly and correctly discover abnormalities in big blockchain networks is highlighted by comparing it to other transaction monitoring tools.

Received: 18.05.2025 Revised: 07.07.2025 Accepted: 22.07.2025

A paradigm based on digital twins is presented for the dynamic management of blockchain systems via real-time simulation of behaviours and settings. This approach integrates predictive analytics, performance modelling, and automated adaptation to enhance blockchain scalability and resilience. Essential components include a system monitor, digital twin controller, and feedback loop [1]. A defence mechanism is proposed for RAFT-based IoT blockchain networks to counteract active assaults, including replay, Sybil, and message manipulation. The approach employs distributed authentication, timestamp validation, and the reinforcement of consensus protocols to reduce hazards. Performance measurements concentrate on packet loss rate, transmission latency, and energy usage under assault scenarios [2]. Crystal implements a quorum certificate-based system to enhance transparency in blockchain mining. The method authenticates block proposals using consolidated signatures and threshold-based certification, therefore reducing uncertainty in block creation procedures. Integration with consensus procedures guarantees uniform perspectives among nodes while averting equivocation [3]. DeFiScope utilises Large Language Model (LLM) reasoning to identify price manipulation attempts in decentralised financial systems. The analysis encompasses sandwich attacks, oracle manipulations, and flash loan vulnerabilities using multi-transaction pattern detection. LLM prompts convert blockchain data into logical restrictions to detect suspicious transactions [4].

BlockSecAnalyzer was used because blockchain platform assaults are becoming more frequent and sophisticated. Attackers targeting transaction processing weaknesses have targeted DeFi protocols and bitcoin exchanges. High-profile fraud, rug pulls, and money laundering occurrences have highlighted the need for enhanced protection. BlockSecAnalyzer automates and scales blockchain transaction monitoring to identify suspicious activity early and reduce financial and reputational risk. The technology detects abnormalities before they become security issues, making the blockchain ecosystem safer and more secure. Section 2 discusses blockchain security and on-chain transaction abnormalities that threaten blockchain ecosystems. Due to its decentralisation, blockchain networks make it difficult to identify fraud, money laundering, and other crimes. Section 3 discusses BlockSecAnalyzer's transaction anomaly detection capabilities. The program employs complex algorithms to analyse transaction patterns, detect suspect behaviour, and provide real-time notifications for further investigation. Section 4 shows how BlockSecAnalyzer has been used in blockchain security frameworks. These examples highlight how the tool has improved security by identifying and preventing harmful activity in real-world blockchain networks. Section 5 concludes with a summary of the results and emphasises the use of BlockSecAnalyzer in blockchain forensics and threat monitoring. It shows how real-time anomaly detection mitigates risks and protects blockchain networks.

ANOMALY TRANSACTION MONITORING

A static analysis approach detects vulnerabilities associated with flash loans in Decentralised Finance (DeFi) systems. The suggested tool analyses Solidity codebases for vulnerabilities related to unsecured lending, swift arbitrage, and governance exploitation. Pattern-matching heuristics and data flow analysis identify transaction re-entrancy, liquidity drain pathways, and pricing oracle misconfigurations [5]. The DeFi'24 symposium emphasises security advancements and obstacles in decentralised financial systems. Principal subjects are cross-chain asset vulnerabilities, formal verification of smart contracts, and the trustworthiness of oracles. Researchers propose approaches for detecting pricing manipulation, modelling economic exploitation, and conducting automated audits [6]. DeFort provides an automated solution for detecting price manipulation threats in DeFi applications via the analysis of transaction patterns and behavioural traces. The essential components are a feature extractor, behaviour classifier, and report generator. The input data includes token exchanges, liquidity contributions, and indicators particular to the protocol [7]. The security attributes of EOSIO-based systems are examined, emphasising weaknesses in smart contracts, systemic threats, and techniques for mitigation. Categories include resource overexploitation, memory corruption, signature falsification, and inter-contract data leakage. The analysis included attack demos, the efficacy of patches, and results from open-source audits [8].

A blockchain architecture based on Directed Acyclic Graphs (DAG) is presented for safe routing in Mobile Ad Hoc Networks (MANETs) connected with Internet of Things (IoT) devices. The design reduces cost by substituting linear chain constraints with DAG parallelism, hence enhancing scalability and route validation. Essential characteristics include timestamp consensus, node trust evaluations, and expedited route switching [9]. A safe routing system, enhanced by blockchain technology, is developed for cluster-based MANETs, integrating cryptographic trust models with decentralised ledger documentation. Nodes provide communication pathways via a synthesis of digital signature authentication and decentralised reputation metrics. Cluster heads preserve route histories and anomaly detection modules while synchronising information on the blockchain [10]. A mechanised

system generates attack transactions for constant product market makers using symbolic execution and exploit-generating algorithms. This tool analyses transaction relationships, assesses attack viability, and generates actionable transaction sequences capable of depleting liquidity or capitalising on slippage. Targets include Automated Market Maker (AMM) smart contracts exhibiting weaknesses in price logic or oracle latency [11]. A contrastive learning approach is proposed for the detection of money laundering inside Bitcoin networks via the analysis of transaction subgraphs. Principal characteristics include structural resemblance, temporal closeness, and address behavioural tendencies. A graph neural network model acquires representations of both regular and suspect transaction sequences [12].

ON-CHAIN EVENT ANALYSIS

A lightweight intrusion detection solution for MANETs is created using blockchain-supported integrity and trust models. The proposed system incorporates a distributed ledger for the storage of anomaly notifications and node behavior records. Intrusion detection modules oversee traffic for blackhole, grayhole, and flooding assaults, while blockchain guarantees tamper-proof event documentation [13]. A blockchain-enabled data aggregation framework is suggested for safe communication in zone-based MANETs, highlighting a risk-aware design. Nodes are organized into zones, with local aggregators tasked with data collecting and encryption prior to uploading information to a blockchain [14]. A blockchain protocol is developed to provide immediate content redaction in permissionless environments while maintaining decentralization. This paradigm incorporates redaction information into blocks and mandates consensus permission for content modifications using voting mechanisms [15]. An investigation based on measurement investigates the operational behaviors of instant cryptocurrency exchanges, concentrating on exchange routing, slippage, and transaction volume. Data is gathered via real-time engagement with prominent quick swap services. Observations include erratic currency rates, absence of clear charge frameworks, and vulnerability to front-running risks [16].

The suggested system uses BlockSecAnalyzer for enhanced blockchain forensics transaction analysis and threat detection. Decentralised apps, tokenised assets, and automated protocols are growing exponentially, making proactive anomaly detection essential for safe and transparent blockchain ecosystems. This technology analyses transaction patterns, smart contract interactions, and value transfers in real time to detect flash loan exploits, sandwich attacks, money diversions, and bot-driven manipulation. Embed BlockSecAnalyzer into blockchain infrastructures to acquire forensic-grade insights into small deviations from normative behaviour for quick incident response and long-term security posture enhancement. Figure 1 shows a block diagram architecture using blockchain symbols to show BlockSecAnalyzer's on-chain transaction anomaly detection. BlockSecAnalyzer receives real-time transaction data from the blockchain network. This fundamental component uses powerful forensic methods to detect suspicious transactional behaviour and dangers. Analysis is divided into anomaly detection and threat categorisation. These evaluations send results to a central alert system that alerts stakeholders via secure dashboards. This architecture emphasises proactive, layered blockchain integrity and threat visibility.

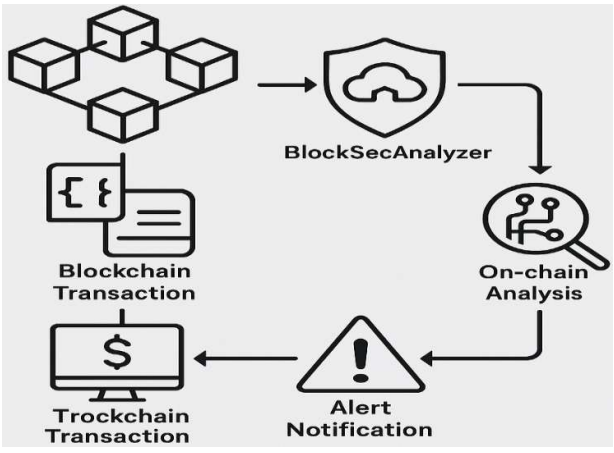

FIGURE 1. Blockchain Anomaly Detection Using BlockSecAnalyzer for Threat Monitoring

Real-time data intake pipelines, anomaly detection models, blockchain state crawlers, and incident response modules form the system's architecture. BlockSecAnalyzer listens to numerous blockchain networks' on-chain events utilising Web3 APIs and RPC nodes. Transaction metadata—sender, receiver, value, timestamp, function signature, and gas characteristics—is retrieved, processed, and compared to dynamic baselines. Figure 2 illustrates BlockSecAnalyzer's on-chain transaction anomaly detection utilising blockchain symbols. Vertical flow begins with the blockchain network sending real-time transactions to BlockSecAnalyzer. These layered forensic methods isolate questionable transaction patterns using behaviour profiling and correlation tests. The threat intelligence section classifies and contextualises verified abnormalities. The last component sends security flags to dashboards or reaction teams via dynamic alerts. A logical and traceable blockchain forensics framework improves transparency and proactive threat control.

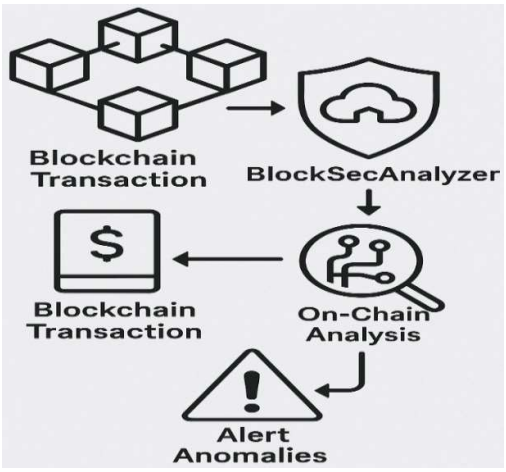

FIGURE 2. Schematic Architecture for On-Chain Anomaly Detection via BlockSecAnalyzer

Smart contract parsers, transaction graph analysis libraries, Apache Kafka stream processors, and TensorFlow and PyTorch machine learning frameworks are used for real-time anomaly categorisation. Front-end dashboards use React.js with D3.js for risk surface heatmaps and interactive contract profiling, while time-series databases record transaction flow metrics. Figure 3 shows a modified workflow model utilising blockchain symbols to illustrate BlockSecAnalyzer's on-chain transaction anomaly detection stages. Blockchain transaction data enters the BlockSecAnalyzer core directly. The module filters questionable activities using pattern recognition and behavioural grading for in-depth forensic examinations. A threat intelligence system identifies threats by severity and origin from outputs.

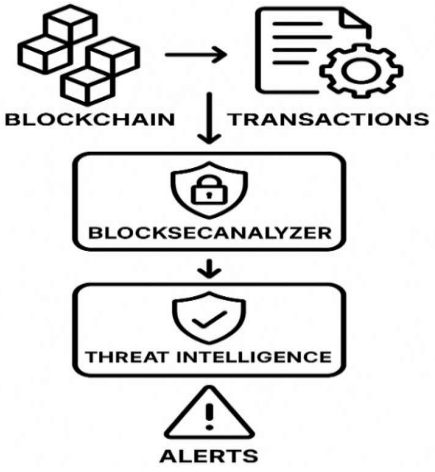

FIGURE 3. Workflow Architecture of On-Chain Anomaly Detection with BlockSecAnalyzer

This system provides sophisticated forensics including cross-contract interaction mapping, token flow visualisation, and changing attack signature threat vector categorisation. BlockSecAnalyzer tracks rogue wallet clusters, transaction replays, and gas spiking/front-running. The method identifies legal DeFi arbitrage from predatory price manipulation using deep pattern recognition and multi-layer correlation. Entities and contracts get dynamic risk evaluations based on on-chain evidence and community-verified notifications. This constantly updating risk intelligence lets ecosystem players prevent, warn, or examine problematic behaviour quickly and clearly.

Figure 4 shows the blockchain security loop in a circular logic design. Blockchain processes create transactions that need verification. Real-time blockchain monitoring assures integrity and compliance for these transactions. Threat intelligence engines contextualise and classify abnormalities and suspicious trends. Loops feed the blockchain for adaptive reactions. High-risk dangers prompt an external alarm system for quick response. Closed-loop blockchain security management is proactive.

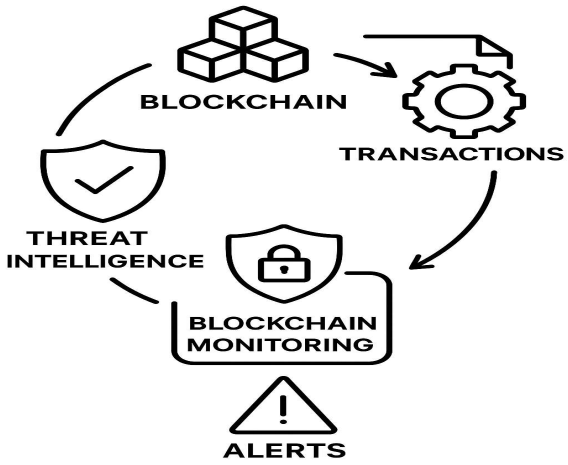

FIGURE 4. Circular Blockchain Threat Detection Loop with Monitoring and Alert Generation

Optimisation balances detection fidelity and resource efficiency. Prioritisation heuristics prioritise high-value assets, key contracts, and highlighted addresses. Vectorised feature extraction and streamlined graph traversal improve processing latency. Cache-assisted model inference speeds up exploit pattern identification, while adaptive learning techniques adjust model thresholds to network-specific activity baselines. Similar transaction group fingerprinting reduces redundant data processing. These optimisations enable scalable deployment without losing analytical depth or responsiveness.

ABNORMAL TRANSACTIONS DETECTION

OpenTracer is designed as a dynamic transaction analyzer to facilitate invariant development in smart contracts. The system analyses Ethereum bytecode to monitor variable states, control flows, and storage changes during contract execution. Captured traces are transformed into potential invariants by symbolic reasoning and data pattern mining [17]. DAppFL is presented as a fault localisation instrument for Decentralised Apps (DApps), using just-in-time trace analysis. The system actively observes execution pathways, records exceptions, and associates error conditions with source code positions. Fault diagnosis is conducted by dependency graph analysis and runtime event clustering [18]. A pre-trained machine learning model is used to identify on-chain attack transactions in Web3 settings, notably focussing on high-frequency harmful activities in mempools. The model employs time variables, gas patterns, and inter-transaction correlations to identify suspicious activities. Benchmarks indicate robust efficacy in identifying sandwich attacks, frontrunning, and flash loan exploits [19]. DAppSCAN generates an extensive dataset of smart contract vulnerabilities inside decentralised application (DApp) ecosystems, facilitating empirical study and tool evaluation. Contracts are retrieved, labelled, and classified according to vulnerability categories, including re-entrancy, integer overflow, and uninitialized storage [20]. The system measures detection delay, true positive rate, transaction throughput, and anomaly correlation

accuracy. Visual dashboards show entity risk timelines, flagged contracts, and real-time alerts. Aggregated views analyse protocol-level risk, while deep drilldowns investigate transactions. Comparing blockchain measurements reveals systemic dangers or distinct behaviours. Performance insights inform detection rule refinement, operational readiness evaluations, and threat intelligence distribution. Figure 5 shows average detection time in milliseconds for BlockSecAnalyzer feature categories and blockchain monitoring stages. Key features like Loop Detection and Contract Calls are in rows, while columns reflect monitoring phases like Input Parsing and Validation Review. The statistics represent how long anomaly detection modules processed each situation. Computational analysis is more demanding with high values.

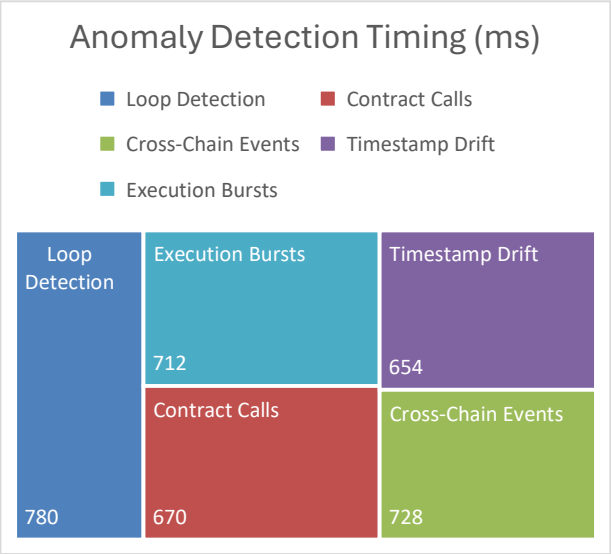

FIGURE 5. Anomaly Detection Timing (ms) by Feature Type and Monitoring Stage

Encrypted data streams, role-based access restriction, and public dashboard redaction of sensitive user identities protect privacy. Explainable AI outputs explain anomaly flags without revealing private key use or wallet balances. Audit trails track all transaction analytics and model operations, and jurisdictional data preservation regulations are adjustable. The technology meets mandated cybersecurity and data handling requirements while maintaining blockchain forensics openness. Table 1 shows a complete BlockSecAnalyzer procedure for on-chain transaction abnormalities. Real-time blockchain transaction records are ingested during Data Ingestion. Sender, recipient, and value information are extracted for specific examination in Feature Extraction. Behavioural Profiling uses previous behaviour to identify transaction sequence irregularities. Alert Triggering records suspicious activity notifications. Finally, Investigation Logging organises all findings into a forensics report. This table clearly shows each technical process without speculation or interpretation.

TABLE 1. Transaction Anomaly Detection Framework Using BlockSecAnalyzer for Blockchain Forensics

Detection Phase	Blockchain Input Stream	BlockSecAnalyzer Unit	Analysis Objective	Monitored Output
Data Ingestion	On-Chain Transaction Records	Blockchain Listener Interface	Real-Time Activity Collection	Parsed Transaction Log
Feature Extraction	Transaction Metadata Fields	Attribute Analyzer Module	Key Parameter Isolation	Structured Metadata Snapshot
Behavioral Profiling	Historical Activity Sequences	Anomaly Pattern Detector	Deviation Mapping	Unusual Activity Pattern Index
Alert Triggering	Correlated Transaction Events	Threat Identification Engine	Suspicious Behavior Recognition	Logged Alert Entry
Investigation Logging	Finalized Detection Outcomes	—	Audit Compilation and Archiving	Blockchain Forensics Report

Mixer utilisation and contract proxying may conceal source-to-destination analysis, limiting it. Genuine but abnormal transaction patterns may imitate exploit behaviours, necessitating human-in-the-loop inspection. Historic transaction variety and relevance determine behavioural modelling accuracy, requiring periodic model retraining. Off-chain information may be needed to attribute harmful activities due to on-chain anonymity. The system monitors decentralised financial behaviour with unequalled openness, speed, and granularity despite these restrictions. Figure 6 shows the frequency of BlockSecAnalyzer alarms for distinct attack vectors using various detection algorithms. Rows represent danger vectors like Front-Running or Flash Loans, while columns list detection techniques like Pattern Matching or Event Correlation. The numbers show analysis alert frequency.

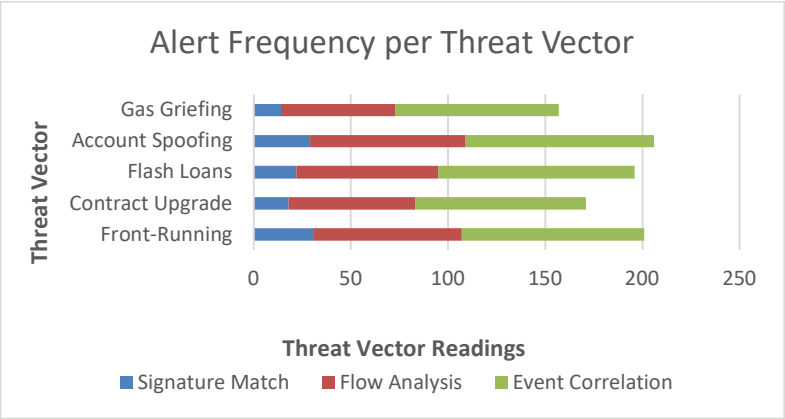

FIGURE 6. Alert Frequency per Threat Vector and Detection Method

In real life, decentralised exchanges monitor frontrunning and liquidity hijacking, DeFi protocols detect flash loan manipulation, NFT platforms detect bot-driven minting, and auditors validate money flows during project assessments. The solution helps regulatory agencies track cash in compliance investigations and gives security researchers a dynamic exploit analysis toolbox. Shared dashboards and annotations let community watchdogs and threat intel partnerships enforce security decentralized. Table 2 shows a structured approach for BlockSecAnalyzer transaction-level anomaly detection. Transaction Capture extracts live on-chain transaction streams for examination. Field Interpretation summarises sender, recipient, timestamp, and value. Inconsistencies are found by comparing transaction flows to predicted behaviours. Risk Mapping matches these results with risk signatures to identify relevant transactions. Report Structuring formalises the findings into a detection report. Each level is technical, without speculation or interpretation.

TABLE 2. Sequential Analysis Model Using BlockSecAnalyzer for Blockchain Anomaly Detection

Processing Step	Input Element	BlockSecAnalyzer Module	Inspection Target	Generated Output
Transaction Capture	On-Chain Data Feed	Capture Interface	Live Transaction Extraction	Ingested Transaction Dataset
Field Interpretation	Transaction Structure Components	Data Parsing Unit	Attribute Identification	Parsed Field Summary
Pattern Analysis	Behavioural Flow Sequences	Anomaly Evaluation Engine	Sequence Deviation Scanning	Irregular Flow Indicators
Risk Mapping	Identified Deviations	Threat Correlation System	Suspicious Activity Linking	Transaction Risk Flags
Report Structuring	Evaluation Summary	—	Findings Compilation and Output	Final Anomaly Detection Report

Zero-knowledge threat proofs, crowdsourced malicious contract labelling, and AI-generated repair solutions are coming. Enhanced zk-roll up and cross-chain bridge capabilities will allow extensive forensics in interoperable ecosystems. On-chain notification hooks and DAO-driven alerts will enable decentralised reaction. With further development, the system might become a central nervous system for proactive blockchain threat detection and safe transactions. This technology helps blockchain stakeholders move from reactive breach reaction to real-time threat anticipation using BlockSecAnalyzer. The basis for safe, transparent, and responsible blockchain operations allows next-generation apps to flourish in a complicated digital ecosystem.

CONCLUSION

BlockSecAnalyzer offers a robust method for detecting anomalies in on-chain transactions, hence improving blockchain forensics via the identification of dubious activity and illicit money transfers. Challenges include the intricacy of distinguishing authentic high-volume transactions from nefarious ones, especially in decentralised settings with many participants. Dependence on previous data and established behavioural models may lead to sporadic false positives or the failure to identify new assault patterns. Notwithstanding these constraints, the tool substantially enhances security operations by providing real-time warnings, transaction analysis, and comprehensive threat monitoring, hence augmenting the resilience of blockchain networks. The use of machine learning models enhances accuracy over time, while the ongoing monitoring capability enables proactive threat mitigation. The future scope entails the expansion of detection algorithms to confront developing risks, the integration of behavioural analytics to minimise false positives, and the improvement of interoperability with diverse blockchain protocols. The integration of BlockSecAnalyzer with extensive blockchain security ecosystems will enhance cooperative threat detection and response across several decentralised platforms.

REFERENCES

[1]. G. Diamantopoulos, N. Tziritas, R. Bahsoon, and G. Theodoropoulos, 2022, "Digital Twins for Dynamic Management of Blockchain Systems," Winter Simulation Conference, pp. 2876–2887.
[2]. H. M. Buttar, W. Aman, M. M. U. Rahman, and Q. H. Abbasi, 2023, "Countering Active Attacks on RAFT-Based IoT Blockchain Networks," IEEE Sensors Journal, vol. 23, no. 13, pp. 14691–14699.
[3]. J. Niu, F. Gai, R. Han, R. Zhang, Y. Zhang, and C. Feng, 2023, "Crystal: Enhancing Blockchain Mining Transparency with Quorum Certificate," IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 5, pp. 4154–4168.
[4]. J. Zhong, D. Wu, Y. Liu, M. Xie, Y. Liu, Y. Li, and N. Liu, 2025, "DeFiScope: Detecting Various DeFi Price Manipulations with LLM Reasoning," arXiv preprint arXiv:2502.11521, pp. 1–16.
[5]. K. W. Wu, 2024, "Strengthening DeFi Security: A Static Analysis Approach to Flash Loan Vulnerabilities," arXiv preprint arXiv:2411.01230, pp. 1–9.
[6]. L. Zhou, and K. Qin, 2024, "DeFi'24: Workshop on Decentralized Finance and Security," Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, pp. 4907–4908.
[7]. M. Xie, M. Hu, Z. Kong, C. Zhang, Y. Feng, H. Wang, and Y. Liu, 2024, "DeFort: Automatic Detection and Analysis of Price Manipulation Attacks in DeFi Applications," Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis, pp. 402–414.
[8]. N. He, H. Wang, L. Wu, X. Luo, Y. Guo, and X. Chen, 2025, "A Survey on EOSIO Systems Security: Vulnerability, Attack, and Mitigation," Frontiers of Computer Science, vol. 19, no. 6, pp. 1–24.
[9]. N. Ilakkiya, and A. Rajaram, 2024, "A novel DAG-blockchain structure for trusted routing in secure MANET-IoT environment," Journal of Intelligent and Fuzzy Systems, vol. 46, no. 3, pp. 5733-5752.
[10]. N. Ilakkiya, and A. Rajaram, 2023, "Blockchain-Assisted Secure Routing Protocol for Cluster-Based Mobile-Ad Hoc Networks," International Journal of Computers, Communications and Control, vol. 18, no. 2, pp. 1–18.
[11]. S. Han, J. Kim, S. J. Lee, and I. Yun, 2024, "Automated Attack Synthesis for Constant Product Market Makers," arXiv preprint arXiv:2404.05297, pp. 1–12.
[12]. S. Ouyang, Q. Bai, H. Feng, and B. Hu, "Bitcoin Money Laundering Detection via Subgraph Contrastive Learning," Entropy, vol. 26, no. 3, pp. 1–24.
[13]. V. R. Sugumaran and A. Rajaram, 2023, "Lightweight Blockchain-Assisted Intrusion Detection System in Energy Efficient MANETs," Journal of Intelligent & Fuzzy Systems, vol. 45, no. 3, pp. 4261–4276.
[14]. V. R. Sugumaran, E. Dinesh, R. Ramya, and E. Muniyandy, 2025, "Distributed Blockchain-Assisted Secure Data Aggregation Scheme for Risk-Aware Zone-Based MANET," Scientific Reports, vol. 15, no. 1, pp. 1–21.
[15]. X. Li, J. Xu, L. Yin, Y. Lu, Q. Tang, and Z. Zhang, 2023, "Escaping from Consensus: Instantly Redactable Blockchain Protocols in Permissionless Setting," IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 5, pp. 3699–3715.
[16]. Y. Hu, Y. Sun, L. Wu, Y. Zhou, and R. Chang, 2024, "Towards Understanding and Analyzing Instant Cryptocurrency Exchanges," Proceedings of the ACM on Measurement and Analysis of Computing Systems, vol. 8, no. 3, pp. 1–24.
[17]. Z. Chen, Y. Liu, S. M. Beillahi, Y. Li, and F. Long, 2024, "OpenTracer: A Dynamic Transaction Trace Analyzer for Smart Contract Invariant Generation and Beyond," Proceedings of the 39th IEEE/ACM

International Conference on Automated Software Engineering, pp. 2399–2402.

[18]. Z. Wu, J. Wu, H. Zhang, Z. Li, J. Chen, Z. Zheng, Q. Xia, G. Fan, and Y. Zhen, 2024, "DAppFL: Just-in-Time Fault Localization for Decentralized Applications in Web3," Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis, pp. 137–148.

[19]. M. B. Koca, and F. E. Sevilgen, 2024, "An efficient index-based algorithm for exact subgraph isomorphism on bipartite graphs," Scientific Research Communications, vol. 4, no. 1, pp. 1-17.

[20]. Z. Huang, D. Tang, R. Zhao, and W. Rao, 2024, "A scientific paper recommendation method using the time decay heterogeneous graph," Scientometrics, pp. 1-25.