AI-Driven Unsupervised Framework for Detecting and Analyzing Anomalous Cryptocurrency Transactions Across Blockchain Networks Using Multi-Feature Analysis

Sri Lestari[1,*], Kiki Setiawan[2]

[1,2]Information System, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, Jakarta Timur,13440, Indonesia

ABSTRACT

The rapid growth of cryptocurrency networks has increased the risk of fraudulent transactions, necessitating effective and scalable detection methods. This study presents an AI-driven framework for detecting anomalous transactions in cryptocurrency datasets using unsupervised learning techniques, specifically the Isolation Forest algorithm. A dataset of 50,000 transactions was analyzed, with 500 anomalies successfully identified based on multiple features including transaction amount, fees, sender and receiver addresses, mining pools, and currency type. The results show that anomalous transactions frequently exhibit extreme values and irregular patterns that are difficult to detect using traditional rule-based approaches. Multi-feature analysis enhances detection accuracy, enabling the prioritization of high-risk transactions for manual review or automated mitigation. These findings demonstrate that unsupervised AI methods provide a robust, adaptive, and scalable solution for proactive fraud detection in blockchain networks, with the potential to integrate deeper learning models for further improvement in detecting complex fraudulent behaviors.

Keywords Cryptocurrency Fraud Detection, Unsupervised Machine Learning, Anomaly Detection, Blockchain Security, Isolation Forest

INTRODUCTION

The rapid expansion of cryptocurrency networks has transformed the financial ecosystem by providing decentralized, transparent, and secure platforms for digital transactions. Despite these advantages, the rise in transaction volume has coincided with increasing occurrences of fraud, including phishing, scams, and manipulative trading activities. These fraudulent activities not only compromise the security of blockchain networks but also undermine user trust and can result in significant financial losses. Detecting such fraud is challenging because transaction patterns are complex, evolving, and often hidden among millions of legitimate operations, making traditional rule-based systems insufficient for real-time detection [1], [2].

Artificial intelligence and machine learning techniques have emerged as promising tools for identifying fraudulent behavior in cryptocurrency networks. Methods such as supervised learning, ensemble algorithms, and anomaly detection models have been applied to detect suspicious transactions. These techniques offer advantages over traditional systems by automatically learning

Submitted: 5 November 2025
Accepted: 15 January 2026
Published: 1 May 2026

Corresponding author
Author name, author@mail

Additional Information and Declarations can be found on page 176

DOI: 10.47738/jcrb.v3i2.67

How to cite this article: S. Lestari and K. Setiawan, "AI-Driven Unsupervised Framework for Detecting and Analyzing Anomalous Cryptocurrency Transactions Across Blockchain Networks Using Multi-Feature Analysis," *J. Curr. Res. Blockchain,* vol. 3, no. 2, pp.113-124, 2026.

patterns from historical data and adapting to changing fraud strategies. Some approaches leverage multi-feature analysis, considering transaction amounts, fees, sender and receiver addresses, mining pools, and currency types to improve the sensitivity of detection [3], [4]. However, most methods require labeled datasets, which are limited in the blockchain domain, and may not generalize effectively across different cryptocurrencies or network conditions [5].

Despite the progress, several research gaps remain in the field of AI-driven fraud detection for blockchain networks. First, many existing models focus on specific cryptocurrencies, such as Bitcoin or Ethereum, limiting the applicability of results to other blockchain systems. Second, most studies do not systematically analyze the interactions between multiple transaction features, which are critical for capturing complex and evolving fraudulent behaviors. Third, the interpretability of AI models remains a challenge, as black-box algorithms often provide limited insights into why certain transactions are flagged as anomalies. These gaps highlight the need for frameworks that are both unsupervised and capable of providing interpretable, actionable insights for mitigating fraud.

This study addresses these challenges by developing an AI-driven framework for detecting anomalous transactions in cryptocurrency networks using unsupervised learning techniques. The framework employs the Isolation Forest algorithm to identify transactions that deviate from normal patterns based on multiple features, without requiring labeled data. By focusing on multi-feature relationships, including transaction amounts, fees, addresses, mining pools, and currency types, the model can detect both extreme and subtle anomalies that may represent fraudulent activity. This approach provides a scalable solution suitable for large transaction volumes and improves the reliability of fraud detection across diverse blockchain networks.

The contributions of this research are threefold. First, it demonstrates the effectiveness of unsupervised machine learning in detecting rare and high-risk anomalies in cryptocurrency transactions. Second, it emphasizes the importance of multi-feature analysis to capture complex patterns of fraudulent behavior that single-feature or rule-based systems may overlook. Third, it provides a framework for practical application in blockchain security, enabling the prioritization of high-risk transactions for automated mitigation or manual review. Overall, this study advances the state-of-the-art in AI-driven blockchain fraud detection by combining robustness, scalability, and interpretability to address the evolving challenges of financial security in cryptocurrency networks.

Literature Review and Related Works

Cryptocurrency networks have experienced rapid growth, which has been accompanied by a significant increase in fraudulent activities. Traditional rule-based systems and manual monitoring methods have proven insufficient to handle the scale and complexity of blockchain transactions, necessitating the adoption of AI-driven solutions [6], [7]. Recent research emphasizes the use of machine learning and deep learning techniques to detect anomalies in transaction patterns, highlighting their capability to identify subtle deviations that are indicative of fraud [8], [9].

Various supervised and unsupervised learning algorithms have been explored for fraud detection in blockchain and digital finance. Supervised models, such as decision trees, random forests, and gradient boosting, rely on labeled datasets to classify transactions as normal or fraudulent, while unsupervised models, including Isolation Forest, autoencoders, and clustering approaches, detect anomalies without requiring labeled data [10], [11]. These approaches allow for real-time identification of suspicious transactions and can scale to handle large volumes of blockchain data, overcoming limitations of conventional methods [12], [13].

State-of-the-art research has integrated hybrid and ensemble learning methods to improve detection accuracy. Ensemble frameworks combine multiple classifiers to leverage the strengths of individual models, effectively reducing false positives and improving sensitivity to rare fraudulent events [14], [15]. Deep learning architectures, such as convolutional neural networks and recurrent neural networks, have been applied to learn complex temporal and spatial patterns in transaction data, enabling detection of sophisticated fraud schemes [16], [17].

Despite these advancements, several research gaps remain. Most existing studies focus on specific cryptocurrencies, limiting the generalizability of the models across multiple blockchain networks [18]. Additionally, few studies systematically analyze the interactions between multiple transaction features, which are critical for capturing complex fraud patterns that involve combinations of transaction amount, fees, addresses, and mining pool behavior [19]. Model interpretability is another challenge, as many AI algorithms function as black boxes, providing limited insights into why a transaction is classified as anomalous [20].

This study addresses these gaps by employing an unsupervised AI framework capable of analyzing multi-feature relationships without relying on labeled data. The approach leverages Isolation Forest for anomaly detection, focusing on features such as transaction amount, fee, sender and receiver addresses, mining pools, and currency types. By combining robust unsupervised learning with multi-feature analysis, the proposed framework aims to improve the detection of rare and high-risk fraudulent transactions, providing actionable insights for monitoring and securing cryptocurrency networks.

Methodology

This study proposes an AI-driven framework for detecting anomalous cryptocurrency transactions using unsupervised learning techniques. The overall research workflow, illustrated in figure 1, consists of sequential stages: data acquisition and preprocessing, feature engineering and normalization, anomaly detection using the Isolation Forest algorithm, and visualization for interpretability. Each stage is designed to capture complex transactional patterns and enable the identification of rare and potentially fraudulent activities in blockchain networks. The figure provides a visual summary of how data flows from raw collection through preprocessing, modeling, and analysis to actionable insights.

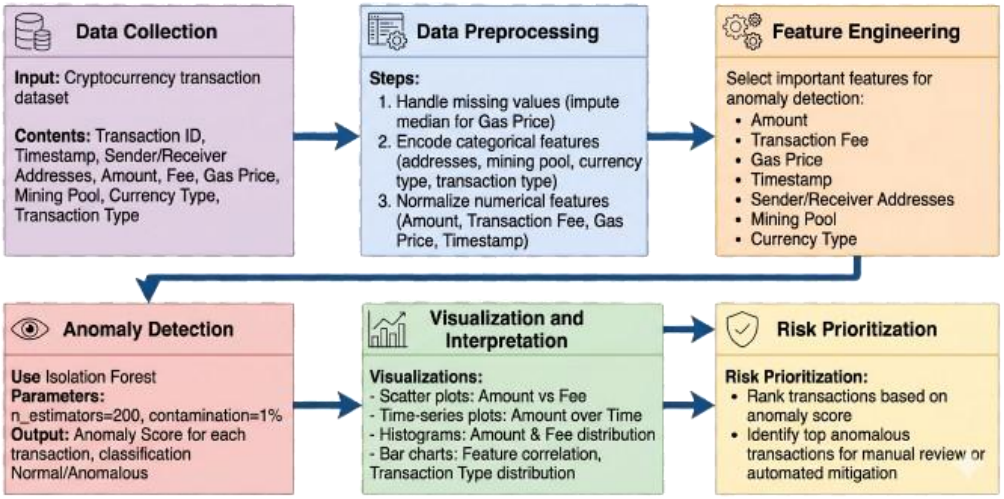

Figure 1 **Research Workflow**

Dataset and Preprocessing

The dataset consists of 50,000 cryptocurrency transactions, including attributes such as transaction ID, timestamp, sender and receiver addresses, transaction amount, transaction fee, gas price, mining pool, currency type, and transaction type. Missing values in the Gas_Price_Gwei feature are imputed using the median to maintain consistency. Timestamps are converted to numeric UNIX format for chronological analysis. Categorical variables, including addresses, block IDs, mining pools, currency types, and transaction types, are encoded using label encoding. Features that uniquely identify transactions, such as transaction ID and status, are excluded to avoid irrelevant influence on the model.

Feature Engineering and Scaling

Feature selection focused on attributes likely to indicate anomalies: transaction amount, transaction fee, gas price, and timestamp. Numerical features are standardized using z-score normalization:

$$z = \frac{x - \mu}{\sigma} \tag{1}$$

$x$is the original feature value, $\mu$is the mean of the feature, and $\sigma$is the standard deviation. This ensures that all features contribute proportionally to anomaly detection, preventing bias from variables with larger scales.

Anomaly Detection Using Isolation Forest

The Isolation Forest algorithm isolates anomalies by recursively partitioning data using random splits. Transactions that require fewer splits to isolate are considered anomalous. The anomaly score for each transaction is computed as:

$$s(x, n) = 2^{-\frac{E(h(x))}{c(n)}} \tag{2}$$

$E(h(x))$is the average path length of transaction $x$across all isolation trees, $n$is

the number of transactions, and $c(n)$is the average path length of unsuccessful searches in a binary search tree of size n. Transactions with scores below a certain threshold are classified as anomalies. The algorithm was trained with 200 trees and a contamination rate of 1 percent.

Visualization and Interpretability

Visualization techniques are employed to interpret model outputs and provide actionable insights. Scatter plots examine relationships between transaction amounts and fees, highlighting clustering of anomalies. Time-series plots show the temporal distribution of anomalies. Histograms and bar charts are used to analyze distributions of amounts, fees, and transaction types, as well as feature correlations. These visualizations allow for a deeper understanding of anomalous behavior and assist in prioritizing transactions for review or mitigation.

Model Evaluation

Even without labeled data, model evaluation is conducted through anomaly proportion, feature correlations, and visual confirmation of extreme or unusual patterns. Anomaly scores are ranked to identify the highest-risk transactions, enabling targeted review. This approach ensures that the framework reliably identifies potentially fraudulent activities in cryptocurrency networks and supports proactive blockchain security.

Results

Detection of Anomalous Transactions

Using the Isolation Forest algorithm with a contamination rate set at 1 percent, the model identified 500 anomalous transactions out of a total of 50,000 cryptocurrency transactions. Each transaction was evaluated based on multiple features, including transaction amount, fee, sender and receiver addresses, mining pool, and currency type. The algorithm assigns an anomaly score to each transaction, allowing for classification as normal or abnormal. In this dataset, the vast majority of transactions, totaling 49,500, were classified as normal, which aligns with the expected proportion of anomalies defined by the contamination parameter. These results are summarized in table 1, which provides a clear overview of the total transactions, the number of anomalies detected, and normal transactions. This demonstrates the model's capacity to handle large datasets while effectively isolating rare events that may indicate fraudulent behavior.

A detailed analysis of the anomaly scores shows that the isolated transactions exhibit unusual patterns compared to the bulk of normal transactions. These patterns include extreme transaction amounts, unusually low or high fees, and irregular associations with certain mining pools or addresses. By detecting these deviations without relying on labeled data, the Isolation Forest provides a robust unsupervised approach to fraud detection in blockchain networks. This capability is particularly valuable in cryptocurrency environments where labeled fraud data is limited and fraudulent activities can occur sporadically across different transaction types and times.

Table 1 Summary of Anomaly Detection

Total Transactions	Anomalies Detected	Normal Transactions
50,000	500	49,500

Visual Analysis of Anomalies

The scatter plot of transaction amount versus transaction fee, shown in figure 2, reveals that anomalous transactions, highlighted in red, are present across both low and high values for amount and fee. Transactions with unusually low fees relative to their amounts may indicate attempts to evade standard processing or exploit network conditions, while those with exceptionally high fees could reflect unusual urgency or manipulation in mining incentives. The clustering of anomalies in regions sparsely populated by normal transactions suggests that these outliers deviate significantly from typical behavioral patterns. These observations indicate that fee structures, in combination with transaction amounts, serve as strong indicators for identifying potentially fraudulent activities, emphasizing the importance of analyzing multiple transaction features simultaneously.

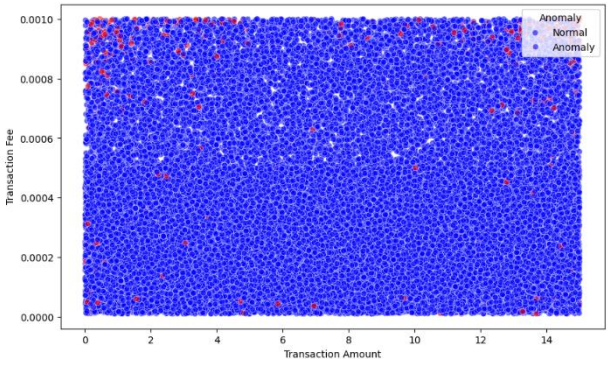

Figure 2 Scatter plot of transaction amount versus transaction fee

The time-series analysis of transaction amounts, as illustrated in figure 3, shows that anomalous transactions occur intermittently throughout the entire observation period with no clear temporal clustering or recurring patterns. Some anomalies appear during periods of low transaction volume, while others are interspersed among normal transactions during peak activity. This sporadic distribution emphasizes the unpredictable nature of fraudulent behavior in cryptocurrency networks and highlights the need for continuous, automated monitoring using robust AI-driven methods.

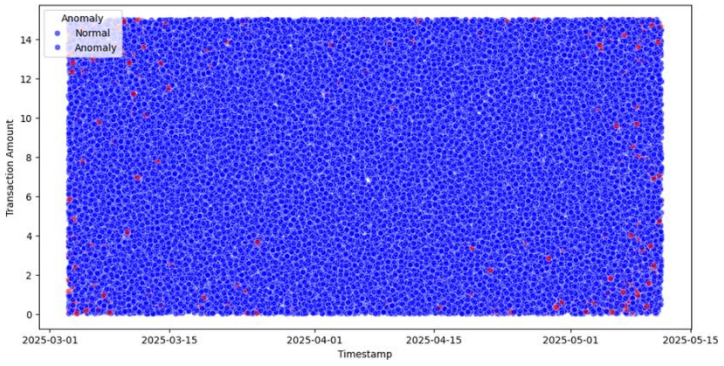

Figure 3 Time-series scatter plot of transaction amounts over time

An analysis of anomaly distribution across different transaction types, presented in figure 4, shows that anomalous transactions are present in nearly all categories, indicating that fraudulent activities are not confined to a single transaction type. This widespread occurrence suggests that attackers exploit various mechanisms within the blockchain network. The fact that only 1 percent of transactions are anomalous reinforces the rarity of fraud events and underscores the importance of AI-driven unsupervised methods capable of identifying subtle deviations from normal patterns across multiple transaction types simultaneously.

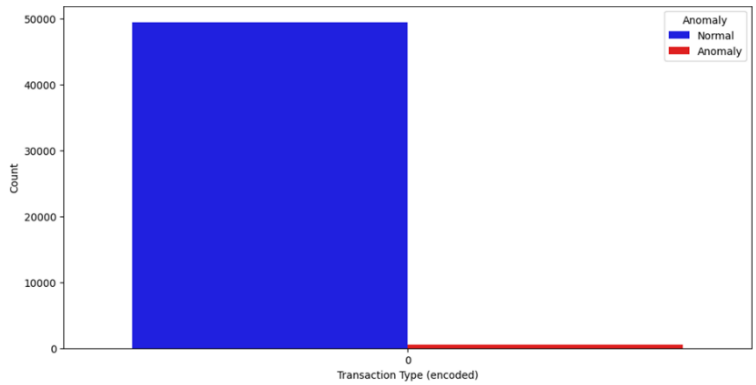

Figure 4 Bar chart showing the distribution of normal and anomalous

Feature Correlation Analysis

The correlation analysis between transaction features and the anomaly score, shown in figure 5, identifies which variables are most influential in detecting suspicious activity. Among all features, Currency, Transaction_Fee, and Receiver_Address exhibit the strongest correlations with anomaly scores, indicating that variations in these attributes are highly associated with deviations from normal behavior. In contrast, Amount and Sender_Address show weaker correlations. These findings emphasize that combining multiple features in the model strengthens the detection of potential fraudulent transactions.

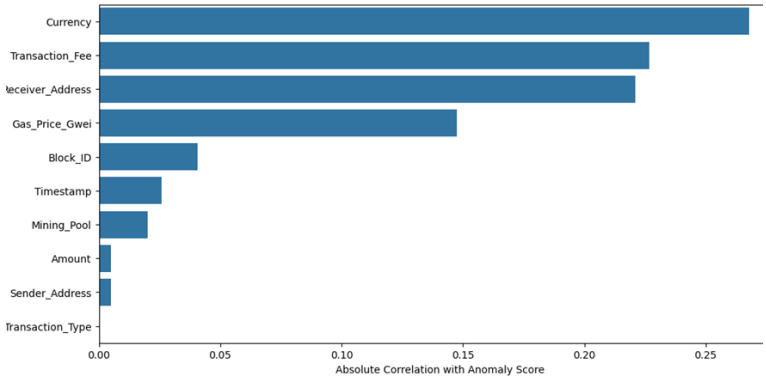

Figure 5 Horizontal bar chart showing the absolute correlation

Distribution of Transaction Amounts and Fees

Histograms in figure 6 illustrate that anomalous transactions tend to occur at the extremes of the amount distribution. Low-value anomalies may represent attempts to conduct micro-fraud or test network vulnerabilities, whereas high-

value anomalies indicate high-risk fraudulent activity, such as transferring unusually large sums. These extreme values are sparsely populated relative to normal transactions, making them visually distinct and statistically significant for detection.

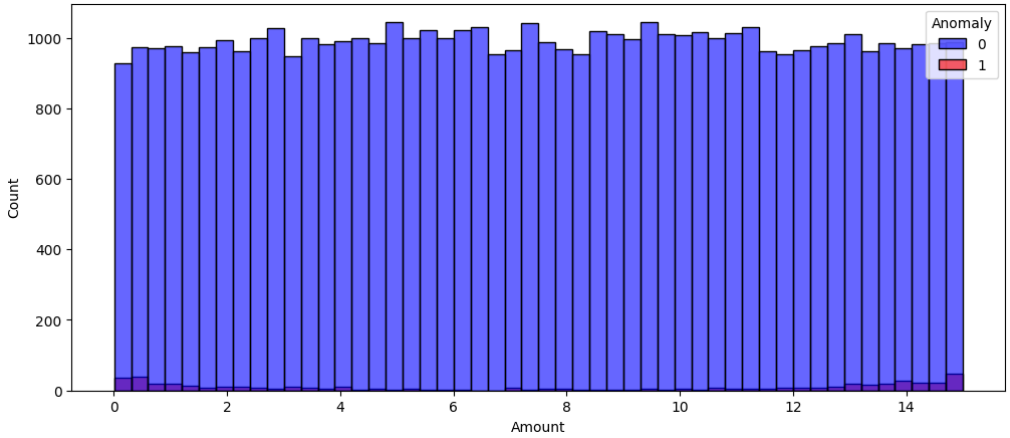

Figure 6 Histogram showing the distribution of transaction amounts by anomaly status

Similarly, the histogram of transaction fees, displayed in figure 7, shows that anomalous transactions often have unusually low or high fees. Low fees may indicate attempts to minimize detection, while high fees can reflect urgency or manipulation of mining incentives. The rare occurrence of these extreme fees among the normal transactions makes them strong indicators of potentially fraudulent activity.

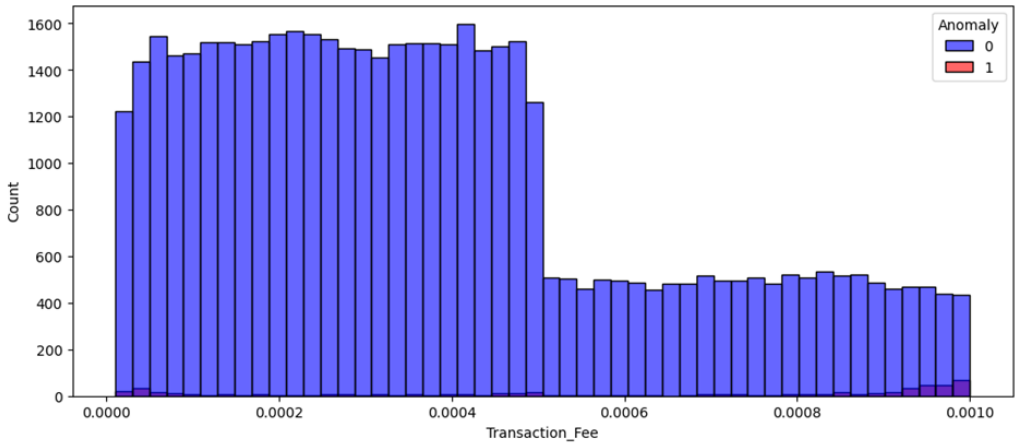

Figure 7 Histogram showing the distribution of transaction fees by anomaly status. Extreme fees correspond to anomalous transactions (red).

Top Anomalous Transactions

The top 10 anomalous transactions, shown in table 2, are ranked by the lowest anomaly scores and include high-value transactions with abnormally low or high fees, often associated with specific mining pools. These transactions are prime candidates for manual review or automated fraud mitigation to enhance blockchain security.

Table 2 Top 10 Anomalous Transactions

Transaction_ID	Amount	Transaction_Fee	Mining_Pool	Anomaly_Score
TXZ21QFKUEDGNS	14.9983	0.000995	4	-0.0361
TXVU6YUKY7WGAI	14.4498	0.000045	4	-0.0352
TX14B4ISCQTU8E	0.4516	0.001000	1	-0.0340
TXYJ9YK71772Y8	8.2161	0.000938	0	-0.0329
TXJ04JV4OKCF2Y	14.9959	0.000999	4	-0.0316
TX04ZTLEAMX4F9	2.3914	0.000945	3	-0.0307
TX7VIT57Q5SAVX	14.7358	0.000076	4	-0.0305
TXVFEVULQEDQSU	14.8987	0.000750	4	-0.0290
TX90EGOLBEQCFJ	13.5082	0.000974	1	-0.0285
TX1W36SKC72QL9	14.8380	0.000093	4	-0.0279

Discussion

The results of this study demonstrate that unsupervised machine learning techniques, particularly the Isolation Forest algorithm, are highly effective in identifying anomalous transactions within large-scale cryptocurrency datasets [21], [22]. The model was able to isolate rare fraudulent events without requiring labeled data, detecting transactions that exhibited unusual patterns such as extreme amounts, unusually low or high fees, and irregular associations with specific mining pools or addresses. These findings highlight the unpredictable nature of fraudulent activity in blockchain networks, which can occur across a wide range of transaction values, at different times, and within various transaction types. The ability to detect these anomalies automatically provides a scalable and robust method for monitoring blockchain networks, especially in environments where ground-truth labels of fraud are scarce.

Further analysis reveals that the interactions between multiple features play a critical role in accurately identifying fraudulent activity. Features such as currency type, transaction fees, and recipient addresses were observed to be the most influential in distinguishing anomalous transactions, while individual features like sender address or transaction amount alone were less predictive. Anomalous transactions often appeared at the extreme ends of the distributions of amounts and fees, suggesting the presence of diverse fraud strategies ranging from micro-fraud or probing activities to high-value manipulative transactions. The identification and prioritization of these high-risk transactions can guide both automated and manual mitigation strategies, improving the overall security and integrity of cryptocurrency networks [23], [24]. Overall, these results reinforce the value of AI-driven unsupervised approaches in providing proactive, adaptive, and scalable solutions for fraud detection in blockchain ecosystems [25].

Conclusion

This study demonstrates that unsupervised AI techniques, particularly the Isolation Forest algorithm, provide an effective and scalable approach for detecting anomalous transactions in large cryptocurrency datasets, allowing for the identification of rare fraudulent activities without the need for labeled data. By analyzing multiple transaction features simultaneously, including transaction amounts, fees, recipient addresses, and mining pools, the model successfully isolated transactions exhibiting extreme or irregular patterns that would be

difficult to detect using traditional rule-based methods. The findings indicate that fraudulent activity in blockchain networks can occur across a wide range of transaction types, values, and times, highlighting the unpredictable and complex nature of cryptocurrency fraud. Incorporating multi-feature analysis enhances the model's ability to capture subtle deviations, enabling the prioritization of high-risk transactions for manual review or automated mitigation, thereby improving the integrity and security of the network. Overall, the results support the adoption of AI-driven unsupervised methods as a proactive, adaptive, and robust solution for monitoring cryptocurrency transactions and mitigating potential fraud, with future work potentially integrating deep learning models to capture even more complex patterns and enhance detection performance.

Declarations

Author Contributions

Conceptualization: S.L., K.S.; Methodology: S.L., K.S.; Software: K.S.; Validation: S.L., K.S.; Formal Analysis: S.L.; Investigation: K.S.; Resources: S.L., K.S.; Data Curation: K.S.; Writing – Original Draft Preparation: S.L.; Writing – Review and Editing: S.L., K.S.; Visualization: K.S.; All authors have read and agreed to the published version of the manuscript.

Data Availability Statement

The data presented in this study are available on request from the corresponding author.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] M. Ul Hassan, M. H. Rehmani, and J. Chen, "Anomaly detection in blockchain networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 289–318, Firstquarter 2023. doi: 10.1109/COMST.2022.3205643.

[2] N. Pocher, M. Zichichi, F. Merizzi, et al., "Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics," *Electronic Markets,* vol. 33, Art. no. 37, 2023, doi: 10.1007/s12525-023-00654-3..

[3] M. Hasan, M. S. Rahman, H. Janicke, and I. H. Sarker, "Detecting anomalies in blockchain transactions using machine learning classifiers and explainability

analysis," *Blockchain: Research and Applications*, vol. 5, no. 3, Art. no. 100207, pp. 1-17, 2024. doi: 10.1016/j.bcra.2024.100207.

[4] G. Airlangga, "Anomaly detection in blockchain transactions: A machine learning approach within the open metaverse," *Jurnal Informatika Ekonomi Bisnis*, vol. 6, no. 2, pp. 308–312, 2024. doi: 10.37034/infeb.v6i2.864.

[5] J. Crisóstomo, F. Bação, and V. Lobo, "Machine learning methods for fraud detection within Ethereum blockchain: A review," *Blockchain: Research and Applications*, vol. 2026, no. March, Art. no. 100469, pp. 1-45, 2026. doi: 10.1016/j.bcra.2026.100469.

[6] C. Cholevas, E. Angeli, Z. Sereti, E. Mavrikos, and G. E. Tsekouras, "Anomaly detection in blockchain networks using unsupervised learning: A survey," *Algorithms*, vol. 17, no. 5, Art. no. 201, 2024. doi: 10.3390/a17050201.

[7] F. Ferdiansyah, U. Ependi, T. Tasmi, M. Haikal, and M. Mikko, "Advanced techniques for anomaly detection in blockchain: Leveraging clustering and machine learning," *Journal of Information Systems and Informatics*, vol. 7, no. 1, pp. 479–492, 2025. doi: 10.51519/journalisi.v7i1.1047.

[8] K. Sankaewtong, T. Kim, C. J. Tessone, and Y. Ikeda, "SoK: Advances in anomaly detection techniques for cryptoasset transactions," *IEEE Access*, vol. 13, pp. 202576–202617, 2025. doi: 10.1109/ACCESS.2025.3636560.

[9] J. Li, Y. Zhang, and C. Yang, "BlockDetective: A GCN-based student–teacher framework for blockchain anomaly detection," *IET Blockchain*, vol. 3, no. 4, pp. 204–212, 2023. doi: 10.1049/blc2.12044.

[10] H. Farrukh, S. Zafar, Z. U. Rehman, A. A. Shah, and N. Alshammry, "Blockchain-based fraud detection: A comparative systematic literature review of federated learning and machine learning approaches," *Electronics*, vol. 14, no. 24, Art. no. 4952, 2025. doi: 10.3390/electronics14244952.

[11] J. Osterrieder, S. Chan, J. Chu, and Y. Zhang, "A primer on anomaly and fraud detection in blockchain networks," *SSRN*, vol. 2023, no. January, pp. 1-24, 2023. doi: 10.2139/ssrn.4317520.

[12] T. T. Pham and S. Lee, "Anomaly detection in Bitcoin network using unsupervised learning methods," *arXiv*, arXiv:1611.03941, 2016. doi: 10.48550/arXiv.1611.03941.

[13] Y. K. Sanjalawe and S. R. Al-E'mari, "Abnormal transactions detection in the Ethereum network using semi-supervised generative adversarial networks," *IEEE Access*, vol. 11, no. September, pp. 98516–98531, 2023. doi: 10.1109/ACCESS.2023.3313630.

[14] Q. Fan, "A survey of deep learning-based methods for detecting anomalous transactions in blockchain," *Science and Technology of Engineering, Chemistry and Environmental Protection*, vol. 1, no. 4, pp. 1-6, 2025. doi: 10.61173/ne7c8839.

[15] N. R. Sidabutar, S. A. Kesuma, F. N. Nasution, and K. Erwin, "Artificial Intelligence, Big Data, and Blockchain Technologies in Financial Fraud Detection: A Systematic Literature Review," *COSTING: Journal of Economic, Business and Accounting*, vol. 8, no. 6, pp. 3865-3874, 2025.

[16] L. P. Krishnan, I. Vakilinia, S. Reddivari, and S. Ahuja, "Scams and solutions in cryptocurrencies—A survey analyzing existing machine learning models,"

Information, vol. 14, no. 3, Art. no. 171, pp. 1-20, 2023. doi: 10.3390/info14030171.

[17] K. Martin, M. Rahouti, M. Ayyash, and I. Alsmadi, “Anomaly detection in blockchain using network representation and machine learning,” *Security and Privacy*, vol. 5, no. 2, Art. no. e192, pp. 1-13, 2022. doi: 10.1002/spy2.192.

[18] J. Li, C. Gu, F. Wei, and X. Chen, “A survey on blockchain anomaly detection using data mining techniques,” in *Blockchain and Trustworthy Systems*, *Communications in Computer and Information Science*, vol. 1156. Singapore: Springer, vol. 2019, no. December, pp. 491–504, 2019 doi: 10.1007/978-981-15-2777-7_40.

[19] T. H. Pranto, K. T. A. M. Hasib, T. Rahman, A. B. Haque, A. K. M. N. Islam, and R. M. Rahman, “Blockchain and machine learning for fraud detection: A privacy-preserving and adaptive incentive based approach,” *IEEE Access*, vol. 10, no. August, pp. 87115–87134, 2022. doi: 10.1109/ACCESS.2022.3198956.

[20] Ferdiansyah, U. Ependi, Tasmi, M. Haikal, and Mikko, "Advanced Techniques for Anomaly Detection in Blockchain: Leveraging Clustering and Machine Learning," *Journal of Information Systems and Informatics*, vol. 7, no. 1, pp. 479-492, Mar. 2025, doi: 10.51519/journalisi.v7i1.1047.

[21] F. T. Liu, K. M. Ting, and Z.-H. Zhou, “Isolation forest,” in *Proceedings of the 2008 IEEE International Conference on Data Mining (ICDM)*, vol. 2008, no. February, pp. 413–422, 2008, doi: 10.1109/ICDM.2008.17.

[22] Y. Witayanont and W. Viyanon, "Anomaly Detection in Bitcoin Network: Using Distance-based and Tree-based Unsupervised Learning Methods," in *Proc. 6th ACM Int. Symp. Blockchain and Secure Critical Infrastructure (BSCI '24)*, Singapore, 2025, pp. 1–7, doi: 10.1145/3659463.3660022.

[23] N. Rathod, M. Karthik, H. Ghongade, J. Shaikh, M. Dhande, R. Deshmukh, and P. Vispute, "Survey of Unsupervised Learning Approaches for Malicious Behavior Detection in Permissionless Blockchain Networks," *Advances in Engineering and Intelligence Systems,* vol. 5, no. 2, pp. 395–410, 2026, doi: 10.22034/aeis.2026.572048.1465.

[24] O. Patel, "Anomaly Detection in Cryptocurrency Transactions Using Machine Learning," *International Journal of Advanced Research in Engineering and Technology (IJARET)*, vol. 12, no. 1, pp. 1266–1282, 2021, doi: 10.34218/IJARET.12.1.112.

[25] V. Pérez-Cano and F. Jurado, “Fraud detection in cryptocurrency networks—An exploration using anomaly detection and heterogeneous graph transformers,” *Future Internet*, vol. 17, no. 1, Art. no. 44, pp. 1-23, 2025. doi: 10.3390/fi17010044.