INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

Cyber Threat Detection and Forensics for Ethereum Cryptocurrency Transactions

Bhairab Sarma[1]*, Anupam Dutta[2], Prazna Lahkar[3], Chayanika Sarmah[3], Sangita Das[3]

1 Department of Computer Science & Engineering, Royal School of Engineering & Technology, The Assam Royal Global University, Assam-781035, India
2 Department pf Mathematics, University of Science and Technology Meghalaya (USTM), Ribhoi District, Meghalaya, India
3 Bachelor of Technology, Department of Computer Science & Engineering, Royal School of Engineering & Technology, The Assam Royal Global University, Assam-781035, India

OPEN ACCESS

Received: 01/07/2026
Accepted: 30/09/2026
Published: 17/10/2026

Citation: Sarma B, Dutta A, Lahkar P, Sarmah C, Das S (2026) Cyber Threat Detection and Forensics for Ethereum Cryptocurrency Transactions. Indian Journal of Science and Technology 19(36): 2496-2503. https://doi.org/10.17485/IJST/v19i36.970

* **Corresponding author**.

sarmabhairab@gmail.com

Funding: None

Competing Interests: None

Copyright: © 2026 Sarma et al. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To detect suspicious fraudulent activities in Ethereum wallet transactions using a graph-based machine learning and anomaly detection techniques. **Method:** From the Ethereum transaction graph, graph structure signals, timing cues, and node level attributes, have been analyzed using unsupervised models like Isolation Forest, Local Outlier Factor, and One-Class SVM to flag irregular wallet patterns. Finally, based on the transaction tracing pattern, illicit transactions are figure out for forensics actions. **Findings:** This work successfully found some suspicious Ethereum wallet behaviors by mixing graph analytics with unsupervised anomaly detection techniques. Graph-based signals such as PageRank, clustering coefficient, transaction frequency and entropy, boosted the capture of strange transaction behaviors that point out as suspicious operation. Isolation Forest did well at isolating the most extreme outliers, while LOF and One-Class SVM highlighted wallets with odd local density, plus a clear behavioral mismatch observed. Overall, the framework worked with the Ethereum transaction dataset from Kaggle, where wallet addresses. Out of 4000 transaction history, top 20 are figure out as may be fraudulent transaction based on their behaviors. **Novelty:** The study integrates graph analytics, blockchain forensics, and unsupervised machine learning to detect anomalous Ethereum wallet behavior without requiring labeled cryptocurrency fraud datasets. Here, only 0.5 percent Ethereum transaction are categorized as suspicious on this study.

Keywords: Blockchain Tracing; Cryptocurrency Transactions; Ethereum; Fraud Detection; Graph Neural Network (GNN)

1 Introduction

Cryptocurrency has come up as one of the most major innovations in the world of modern digital finance, second after Bitcoin [1]. It is a distributed ledger technology and can be referred to as a distributed database since it exists over a computer network [2]. In traditional financial systems, monitoring and detecting suspicious behaviors in transactions happening between two or more accounts was not possible. Today, technology has become the hotspot for many criminals to perform fraud transactions. This is because of the pseudonymity only in block chain network [3]. Due to these illicit activities, the detection and prevention of fraudulent activities is now becoming a necessity task. For the solution of this kind of nuance abnormal transactional flows, there is a need to adapt advanced analytical frameworks.

The graph-based analysis is one impactful solution for detection of illicit activities in the blockchain environment [4]. Graph theoretic methods [5], such as centrality, clustering coefficient, in degree, and out degree, page rank, and k-core number offer key insights into the structure of blockchain transactions. Unsupervised learning has been used in [6] for detecting malicious wallets because there is no labelled data. This study is mainly concerned with Ethereum blockchain owning to its complicated structure, its use of smart contracts, DeFi token exchange, and Non-Fungible Tokens Market Places, additionally implementing graph-based analysis in classification will be utilized.

Traditional financial institutions operate with cash, bank accounts, and other paper-based procedures. However, in global trading, e-commerce, and online services outpace traditional transactions. Cryptocurrencies, such as Bitcoin or Ethereum, are digital tokens and decentralized system that verifies transactions through networks rather than traditional institutions. The decentralization, transparency, and inclusion make it possible to conduct business more efficiently in the era of automatization and connectivity.

The objectives of this study are to:

1. Design and implement a model for detecting fraudulent Ethereum transactions and anomaly detection.
2. Identify abnormal behavior of Ethereum wallets based on graph theory and their structural features.

The concept of blockchain was proposed by Satoshi Nakamoto in the year 2008 [7]. Digital transactions can take place without the presence of a trusted third party with the aid of blockchain technology. In this representation, nodes with most power produce the longest chain and thus become immune to any attacks [8]. In 2013, Vitalik Buterin proposed Ethereum [9], which is now become the second largest digital transaction, extending blockchain capabilities by building a blockchain with a built-in Turing-complete programming language capable of executing smart contracts.

Ouyang *et al*. (2024), in their study [10] applied a Graph Convolutional Networks (GCN) in the Elliptic dataset for anti-money laundering compliance in Bitcoin to see whether a graph deep learning model handles millions of transactions within bitcoin's unique Unspent Transaction Output (UTXO) structure, thus the integration of graph deep learning into blockchain analytics required large labeled datasets for training. Along with UTXO and GCN (Ouyang), Nadia *et al*. in [11], used another Transaction Subgraph Networks (TSGN) to capture complex multi hoping structural behavior which was similar with Chen and Crisostomo. Another unique method, called parecium was used in [12] as a biased random walk algorithm, which is a method to detect scam behaviors on Ethereum. From this above study, it may understand that no deep learning models are required to capture its behavioral patterns, only graph traversal techniques are required. Also, there is a lack of focus on graph-based anomaly detection.

1.1 Supervised Methods

Supervised models are those models that use labelled dataset to train the model to detect illicit behavior. GNN in fraud detection is Temporal Transaction Aggregation Graph Network (TTAGN) by H. Kanajashi [13] and Liu Papan et al., [14]. This integrates GNN with temporal and structural properties to capture transfer activities through time and consumes memory resources and has a simple architecture.

1.2 Unsupervised Methods

Unsupervised methods are those methods that do not require labeled data. Tiyani et al. (2023) introduced Anti Benford Subgraphs which is an unsupervised anomaly detection approach. In the next year, Wang (2022) described how to tackle transaction data irregularities using Bagging Multi-edge Graph Convolutional Network (BM-GCN) [15]. Since fraud detection in Ethereum data lacks on having an unlabeled dataset so in this study unsupervised approach has been used.

1.3 Research Gap

From the above review, upon observation, many pros and cons have been open-up. Few of the major lacking are noted below:

1. The deep analysis of structural wallet behavior with the help of graph theory is not much focused in the existing blockchain studies.
2. Real-world labelled fraud data is hard to obtain and is very limited. This restricts the deployment of supervised approaches in detecting fraud in cryptocurrency.
3. Several approaches mentioned in the papers focus only on transaction amounts and frequencies and often ignore the importance of wallet interaction patterns.
4. For identifying suspicious wallet behavior, the use of graph-based anomaly detection methods is limited when it comes to Ethereum, which has different and unique transaction characteristics.
5. In Ethereum networks, for node-level anomaly detection lack of comprehensive feature engineering can be seen that combines statistical, temporal, and topological features.

In this paper, we tried to mitigate these pitfalls and reduce the mentioned research gaps using graph-based analytical method.

2 Methodology

The complete process of this study is confined with four sub-tasks: data collection, data pre-processing, features engineering and anomaly detection. Collected transactions are represented as a graph structure where wallet addresses are denoted as node and the transactions are denoted by arch. Traversing this graph,

transaction behavior studied by mentioned parameters and suspected as fraud or illicit upon observations.

2.1 Date Collection

Dataset consisting of Ethereum transaction records *(Ethereum Transactions for Fraud Detection. (first_order_df.csv))* has been collected from Kaggle database. This dataset consists of raw transactions that is used to analyze suspicious activity that contains the following columns- **Transaction Hash (Tx Hash), block number (Block Height), timestamp, sender and receiver addresses (From/To), transferred value (ETH), and execution status (is Error, where, 0 = success and 1 = failure)**. The dataset is used for detecting abnormal patterns such as unusual transaction flows or high-frequency activity, forming the basis for graph-based anomaly detection and fraud analysis (Figure 1). Role of each header is discussed below:

TxHash: Transaction Hashis a unique, 66-character cryptographic string value serves as the permanent digital fingerprint for that specific transaction. There are 102149 unique values (as per Kaggle dataset).

BlockHeight: The Block Height is a sequential block number transaction that is grouped, recorded and permanently validated by the network validators.

TimeStamp: Time Stamp is written in Unix epoch time format which time-series and behavioral mapping it is essential.

From: The sender's Ethereum address. With the help of this column models can calculate node's incoming degrees.

To: The receiver's Ethereum address.

Value: The amount of Ether transferred in the transaction.

Is Error: Indicates whether the transaction is a binary 0 for no error, and 1 for error, Transaction failed.

2.2 Data Preprocessing

Data preprocessing cleans and structures raw data by removing duplicates, inconsistencies in temporal information, and incomplete or missing attribute values and entry fields, irrelevant information. To overcome these challenges, a rigorous preprocessing framework is designed and implemented through a specialized class named Ethereum Preprocessor class.

The data preprocessing pipeline consists of five consecutive steps.

2.3 Schema Enforcement

In the very first step the presence of all required columns that is Tx Hash, From, To, Value, Time Stamp, and is Error is verified. The Ethereum wallet addresses (From/To) are normalized converting to lowercase since Ethereum addresses are case-insensitive leading or trailing. Whitespaces of the wallet addresses are stripped. This ensures the same wallet address indicates to a single canonical node in the transaction graph, even if represented in check summed EIP-55 format or lowercase.

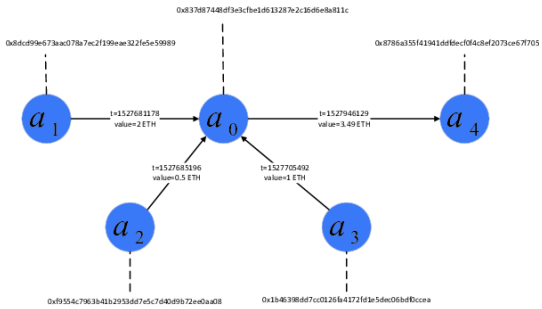


Fig 1. Ethereum graph network (designed by Lie Wang)

Now, each normalized sender and receiver wallet addresses (From/To) are validated against the standard Ethereum hexadecimal structure (0x followed by 40 hexadecimal characters):

$$\backslash 0x\left([a-f,A-F,0-9]\{40\}\right)\$$

Wallet Addresses that fail conform to this pattern or missing vital keys are discarded from the dataset. This step prevents the introduction to phantom nodes in the Ethereum transaction graph that can distort centrality and degree-based features.

Type coercions are applied after address validation.

Value field: Cast to numeric (float) type. Non-numeric values are coerced to NaN.

Time Stamp field: Converted from Unix timestamp, representing seconds since 1970-01-01T00:00:00Z, to datetime format.

Is Error field: Cast to a binary integer type(0/1).Rows with missing values or NaN values in critical columns like TxHash, From, To, Value, or Time Stamp are dropped as incomplete transaction records are not reliable in graph construction. Table 1 lists the Temporal and Value Distribution Feature.

2.4 Features Engineering

The following three modular classes are used for feature engineering:

- For basic transaction statistics, Node Feature Engineer class
- For temporal and distribution features, Temporal Value Feature Engineer class
- For graph topology features, Graph Topology Feature Engineer class

Basic Transaction Statistics (Node Feature Engineer): The feature helps capture how active a wallet behaves. A combination of large max and low average transaction amounts can point to some sort of irregularity may be a scam, phishing, or Ponzi scheme wallet.

2.5 Temporal and Value Distribution Features (Temporal Value Feature Engineer)

Temporal and Value Distribution Features has been described in Table 1:

2.6 Anomaly Detection

The detection of suspicious wallets for illicit addresses is extremely scarce, often incomplete, and hard to collect. The goal of the system is to flag addresses which deviate significantly from the majority of the normal behavior patterns without any prior label. Among all, three models have been used in this work, as stated below:

2.7 Isolation Forest

The model isolates outliers that are structurally isolated from the majority of the data using random decision splits. In a tree, ensemble of size n, the anomaly score s(x, n) for a point x is based on the average path length $E[h(x)]$ over all trees is as given:

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

Table 1. Temporal and Value Distribution Feature

Features	Name	Represent
Count of transaction	out_tx_count	Total number of transactions sent
	in_tx_count	Total number of transactions received
Total Transaction value	out_total_value	Total ETH sent
	in_total_value	Total ETH received
Mean, maximum, and minimum transaction values	out_avg_value	Average outgoing ETH value
	in_avg_value	Average incoming ETH value
	out_max_value	Maximum outgoing ETH value
	in_max_value	Maximum incoming ETH value
	out_min_value	Minimum outgoing ETH value
	in_min_value	Minimum incoming ETH value
Number of unique counterparties	out_unique_counterparties	Number of distinct outgoing addresses transacted with
	in_unique_counterparties	Number of distinct incoming addresses transacted from
Error Ratio of transactions	out_error_ratio	Proportion of outgoing transactions with errors
	in_error_ratio	Proportion of incoming transactions with errors
	in_error_ratio	Proportion of incoming transactions with errors

where,

- h(x)= path Length of point x in an isolation tree.
- $c(n) = 2H(n-1) - \frac{2(n-1)}{n}$ is the average path length of an unsuccessful search in a Binary Search Tree.
- $H(i) = lni + \gamma$ (Euler's constant)

Interpretation.

s≈1 highly anomalous,

s≈0.5 normal,

s<<0.5 very normal.

Here, a threshold at the 99th percentile of IF scores, approximately 0.149. It is used to identify the top 1% of addresses (score > 0.149) highly suspicious candidates for manual investigation.

2.8 Local Outlier Factor (LOF)

Outliers are the points that have sparsity than their neighbors. Local Outlier Factor gets the anomaly score by comparing the local reachability density of a point to the average local reachability density of its k nearest neighbors.

2.9 Precision @K

Precession of the model is measured with the formula for is as given below:

Let:

- $Top_k = setofKaddresseswiththehighestanomalyscores.$
- $Malicious_{confirmed} = subset\ of\ Top_k\ that\ are\ manually\ verified\ as\ fraudulent/scams$

$$Precision@K = \frac{|Top_k \bigcap Malicious_{confirmed}|}{K}$$

With this setup, 4k (approx..) transactions has been downloaded and converted into a graph structure, and based on the features (Table 1), analyzed the transaction path as described in the following section.

3 Results and Discussion

From the 4k data set (downloaded from Kaggle), for each node indegree and outdegree values are calculated based on Ethereum transmitted and received from/to another node. Ethereum value is also accounted to categorize transaction cluster. Some transactions are found very irregulars, sorted them and consider only top 20 transaction for analysis (Figure 2). Using unsupervised machine learning algorithm (Node2Vac), one class SVM have been calculated. A One-Class Support Vector Machine **(One-Class SVM)** is an unsupervised anomaly detection algorithm. It learns the boundary of normal data and identifies points that lie outside this boundary as anomalies. For Ethereum transaction analysis, One-Class SVM can be used to identify suspicious wallets or abnormal transaction patterns without requiring labeled fraud data.

Top 20 addresses and their Etherscan / behaviour labels:

address	one-class svm (ocsvm)_score
0x81c010cf17c4f811de17fc930e17ca63f6a49686	0.002026
0xc5a3c849a80f7ccb88c403e6b491121d0fd789b5	0.002017
0x4f0bde05f4035e79b91e7b85aee2840d12041fa8	0.001993
0xc5a1b86bfe648cb1d5046227c88dd0f77816fb82	0.001963
0x574388f6ab9aad12b151e0d0cb8056234d9f5964	0.001808
0x30ff204347761611d74621005c3004e8ac971c09	0.001565
0x34acb2f40a618b588fc3421290159ecfd92e7a2c	0.001519
0x4ceef27bbda518eb758f511bf1d029ec12652a82	0.001277
0x79aa79116c24a715b5eb1287af8a16201450c895	0.001271
0x14944031371 59bb0dc545d11963fdf797ea1ecab	0.001230
0xb649707891364e5529ce7bcfba463211eb758745	0.001064
0x4eb65966c5f93416af5ad74f60ee1e7873ea026e	0.000947
0xbe37a38a42f17ae06cb1bf4dfa456e9bcdb70148	0.000933
0xf6375f270b2b7b1049d486cb7225abff7d78af34	0.000856
0x3b1f6d7881a459f00a82583852c41109a1e9600c	0.000838
0x2220abd2c871bb61e42cabd9bd6c94a27a920c52	0.000795
0x313932b03c808df52c9a15e561dc0244ed1bce81	0.000776
0xb59550265f83570da30a4da86dc03424cd0c2495	0.000776
0x204fe6dab1e53fa645887106907d7a6ac39013e4	0.000776
0x0ce081bef120aa3392bb75132ba15799d2bfbc90	0.000776

Fig 2. Transaction patten analysis using Node2Vac algorithm

No significant transactions have been observed in this dataset as the lowest OCSVM score closes to zero but positive (not negative). Although these scores are approx. to zero, they are far apart from +1 and considered as suspicious. Accordingly, their Local Outlier Factor (LOF) have been analyzed. LOF features of the same data set are depicted in Figure 3.

Here, Euclidian distance has been counted among nodes and computed marginally stable transactions[16]. As the LOF approaches 2 or more, it seems to be suspicious or fraudulent (outlier). From the analysis, LOF score of transaction 1 is unexpectedly rising (6 points) from the next higher value. The normal ranges spans 10052-17383, with uniform deviation within all 19 transactions whereas 20th transaction (top row in Figure 3) deviation is remarkable.

Finally, precision of the model is observed with different values of K (multiples of five) and measured the value of three model parameter (Table 2). A brief comparison among all three adopted models, isolation forest, LOF, and One-classed SVM is given in Table 2.

Top 20 addresses and their Etherscan / behaviour labels:

address	local outlier factor (lof)_score
0xcb515d908e72dd0e3793d285f4c8208cf0dd592d	72829.158143
0xbab5bc04de51130c0979b9265d682a2e33ca22ce	17383.500528
0x090c859d724e9e678fca8eab7243c218e700fbd9	17261.658420
0xa2d58bd10ee6ee27fd318dc4ab95e7c7509de109	14192.713881
0x7667ee7d212344c3d4e3c88b57da22e40ec56b10	13999.403291
0x524e4374ffb1228d9ae332bd54deeeb51c50be3c	13886.160353
0xd060fad1f0c034782c8ff0c479561b86fa81cb84	13882.586367
0x6f51382de43471e6056864cb39123ac877c1902b	13875.285710
0x486d22d2d7656e2bee93b07fa0befd4ff1c85fc5	13852.179150
0x66655cdaf96cd552da0207401fe78605ffeebe14	13814.766478
0x6e286936b8211905a63725b89bdcbe7229664cb0	13814.723077
0xdea52cc651a7a60e6d43366950c246853d1af626	13767.058801
0xda7fffeef23c75abf7b989417e8d5733af35c067	13765.902699
0x2e69734771a8d36558e0e54cf8a7150a564558c3	13295.988328
0x6a7b5ec0a47939ac8f848be27206a11eb5e0b168	12097.721496
0x047426040f62848dc43c7bc02ad1eb64d276bc2f	10607.243307
0x015414ecd2514bba6fd03618578ba5164e1e63a4	10479.520114
0x92f6c026a533c268121499c9f9624d923b70d3f7	10406.836770
0x2b12d1d310c6df937c8c56b7a1a34ebea63529ac	10405.148936
0x4b2e978d8503c56534ab4f79130e8932af429258	10052.343965

Fig 3. LOF value of suspicious transactions

Table 2. Parametric variation of Precision with value of K in multiples of 5

Value of K	Isolation Forest (IF)	LOF	OCSVM
5	0.5956	0.4107	0.5998
10	0.2988	0.2959	0.4780
15	0.3334	0.3207	0.3200
20	0.4447	0.45000	0.2607

From the above experimental results, it analyses that with minimum value of K, IF score approaches higher values corresponding to LOF and OCSVM. Anomaly can be detected (suspected) based on variation of these three parameters variation. In our experiments, from the to 20 suspicious transaction, only top 2 transaction can be brought under consideration of further analysis. As compared to previous models **(Becao & Chen),** where multilayer topological graph structure has been used to study suspicious behaviors, we provide a novel architecture of a homogeneous graph structure through which suspected transaction can be isolated for further review. Our model verified a transaction with multiple dimensions like time, amount and depth of tree for link analysis. Further it can be utilized to detect the original source of fraudulent transaction which have not observed in earlier models. In addition, a Features Gated temporal graph learning (FG-EGCN) method, proposed by Han et. al.[17] for illicit Bitcoin transaction detection and investigation can be used to address many practical challenges in transaction. FG-EGCN combines temporal graph encoding with a residual feature branch and a feature-gated fusion mechanism, introduces a focal-loss-based optimization to improve understanding of rare illicit transactions.

4 Conclusion

This study presents a novel graph-based machine learning approach with the following pipeline: data preprocessing, feature engineering, temporal splitting, and unsupervised anomaly detection. Isolation Forest and LOF got similar value at Pricision@20 i.e 44%. However, the Precision@5 is 59% for Isolation Forest and 40% at Precision@5. This means that the prediction done by the Isolation Forest is more reliable. Precision@5 for OCSVM 59% but by Pricision@20 it drops sharply to 25%, worst among the three. Thus, Isolation Forest is the most balanced and practical model followed by LOF, however OCSVM is unsuitable for unsupervised anomaly detection. Further, it has been revealed that based on graph nature, one cannot determine perfectly a fraudulent transaction, instead it may come to closure monitoring for considering as a suspicious nature. There needs more sophisticated analysis to fine the original source and destination addresses which are played suspicious behavior. This study only analysis graph features to detected suspicious transaction, however, for taking precaution measure, next level enhancement in the algorithm would be required.

5 Acknowledgements

The authors thank their institutions for providing the necessary facilities and support.

Author details: Bhairab Sarma and Anupam Dutta are Associate Professors; Prazna Lahkar, Chayanika Sarmah and Sangita Das are Bachelor of Technology.

References

1) Crisostomo J, Bacao F, Lobo V. Machine learning methods for fraud detection within Ethereum blockchain—A review. *Blockchain: Research and Applications*. 2026. https://doi.org/10.1016/j.bcra.2026.100469.
2) Chen Y, Zhang Y, Chan S, Chu J, Lord N. Multilayer topology-aware graph contrastive learning for fraud detection in the Ethereum transaction network. *Journal of the Royal Statistical Society: Series A (Statistics in Society)*. 2026;189(2). https://doi.org/10.1093/jrsssa/qnaf135.
3) Zhang Y, Liu P, Wang G, Li P, Gu W, Chen H, et al. GTSF: A novel Ethereum phishing scams detection method based on gaining transaction semantics features. *Expert Systems with Applications*. 2026;307. https://doi.org/10.1016/j.eswa.2025.130950.
4) Gandhi M. Fraud Detection in Blockchain Transactions Using Graph-Based Deep Learning. *PUXplore Multidisciplinary Journal of Engineering*. 2025;1(1). Available from: https://puxplore.paruluniversity.ac.in/index.php/PXMJE/article/view/2.
5) Adam T, Babič F. Identifying illicit activities in blockchain transaction graph networks. *Electronics*. 2025;14(23). https://doi.org/10.3390/electronics14234599.
6) Ghnemat R, Mosa H. Blockchain-based fraud detection: A systematic review of Ethereum network applications. *Cluster Computing*. 2025;28(3). https://doi.org/10.1007/s10586-025-05797-w.
7) Han B, Wei Y, Wang Q, Collibus FMD, Tessone CJ. MTAD: Multi-layer Temporal Transaction Anomaly detection in Ethereum networks with GNN. *Complex Intelligent Systems*. 2024;10. https://doi.org/10.1007/s40747-023-01126-z.
8) Siftee R, Ghosh M, Baliyan N, Rashmitha MJ, Singh S. Graph neural network based phishing account detection in Ethereum. *The Computer Journal*. 2024;67(12). https://doi.org/10.1093/comjnl/bxae079.
9) Sun J, Jia Y, Wang Y, Liu Y, Sheng Z, Tian, et al. Ethereum Fraud Detection via Joint Transaction Language Model and Graph Representation Learning. *arXiv Research Paper*. 2024. https://doi.org/10.48550/arXiv.2409.07494.
10) Ouyang S, Bai Q, Feng H, Hu B. Bitcoin Money Laundering Detection via Subgraph Contrastive Learning. *Entropy*. 2024. https://doi.org/10.3390/e26030211.
11) Nadia P, Mirko Z, Fabio M, Muhammad ZS, Stefano F. Detecting Anomalous Cryptocurrency Transactions: An AML/CFT Application of Machine Learning-Based Forensics. *Scientific Reports (Springer Nature)*. 2023. https://doi.org/10.48550/arXiv.2206.04803.
12) Tianyi C, Tsourakakis CE. AntiBenford Subgraphs: Unsupervised Anomaly Detection in Financial Networks. *IEEE / ACM Conference Proceedings*. 2023. https://doi.org/10.48550/arXiv.2205.13426.
13) Kanezashi H. Detection with Heterogeneous Graph Neural Networks. *IEEE Conference Proceedings*. 2022. https://doi.org/10.48550/arXiv.2203.12363.
14) Li P, Xie Y, Xu X, Zhou J, Xuan Q. Phishing Fraud Detection on Ethereum using Graph Neural Networks. *IEEE Conference Proceedings*. 2022. https://doi.org/10.48550/arXiv.2204.08194.
15) Wang J. TSGN: Transaction Subgraph Networks Assisting Phishing Detection in Ethereum. *arXiv Research Paper*. 2022. https://doi.org/10.48550/arXiv.2208.12938.
16) Liu Z, Chaochao C, Xinxing Y, Zhou J, Li X, Song L. Heterogeneous Graph Neural Networks for Malicious Account Detection. *arXiv Research Paper / IEEE-related Conference Paper*. 2022. https://doi.org/10.48550/arXiv.2002.1230.
17) Han N, Zhang R, Liu X, Zhang H. Illicit Bitcoin transaction detection via feature-gated temporal graph learning. *Scientific Reports*. 2026;16. 22352. https://doi.org/10.1038/s41598-026-53783-y.