Journal of Multidisciplinary Engineering Science Studies (JMESS)
ISSN: 2458-925X
Vol. 12 Issue 4, April - 2026

Anomaly Detection In Cryptocurency Using Unsupervised Learning Techniques: A Comparative Analysis Of Different Models

Olusola S. Olatunji [1]
Department of Computer Engineering
Federal University of Technology,
Akure, Nigeria.
Olatunji84olusola@gmail.com

Eratus O. Ogunti [1]
Department of Computer Engineering
Federal University of Technology
Akure, Nigeria.
oguntig@gmail.com

Osekhonmen V. Abhulimen [2]
Department of Information and
CommunicationEngineering,
Elizade University, Nigeria.
osekhonmen.abhulimen@elizadeuniversity.edu.ng

***Abstract*—The growth of decentralized cryptocurrency networks such as bitcoin has created opportunities for illicit activities which include fraud, money laundering and market manipulation. A major challenge in securing cryptocurrency network is detecting anomalies in the network because cryptocurrency dataset are unlabelled. This research addresses this problem by developing and evaluating a framework for anomaly detection in the bitcoin network using unsupervised learning techniques. The methodology employed a dual graph representation, constructing both user graph and transaction graph from public bitcoin data acquired from BigQuery database. Graph based neural network architectures such as Graph Convolutional Network Graph Autoencoder (GCN-GAE) and the Graph Attention Network Autoencoder (GAT-AE) and classical algorithms, such as One-Class Support Vector Machine (One-Class SVM) and Isolation Forest were trained and implemented. The performance of the models was evaluated using a combination of quantitative metrics, which includes Silhouette Score for embedding quality and Mean Dual Evaluation (mDE) metric to assess cross graph consistency. The findings reveal that GCN-GAE perform highly with distinct embeddings having Silhouette score of 0.922 for user gtaph. Also, GCN-GAE has a strong Silhouette score of 0.691. The GAT-AE excelled at detecting anomalies across both user and transaction graphs (mDE = 0.251).**

Keywords—Cryptocurrency; bitcoin,bigquerry; unsupervised learning;deep learning ;

I. INTRODUCTION

Network structures have appeared for a long time and along with them are those who behave abnormally within the system.These people or their illegal activities are refered to as anomalies. With respect to financial transaction networks, anomalies can include those who execute fraudulent transactions. In these net works, a common goal is to detect those anomalies to prevent future illegal actions in cryptocurrency network.

Cryptocurrency refers to a digital payment system that operates similarly to the standard monetary currency system and allows users to send and receive virtual payments outside of traditional financial institutionsand offer low transaction costs and a peer-to-peer system. [2]

The decentralization of cryptocurrency has been a key factor in the enhancement of user privacy and provides various levels of anonymity [1] .

Bitcoin was the first decentralized blockchain based cryptocurrency and continues to be the most widely used cryptocurrency in the market .

This research seek to detect anomalies or suspicious activities in this anonymous network, where nodes(that is users, transactions) are unlabelled and there is no confirmation as to whether or not a given node is actually conducting illicit activities.

The research will focus particularly on the problem of detecting anomalies in the bitcoin transaction network, which is related to the study of fraud detection in all types of financial transaction systems in which a large literature exists.

II. LITERATURE REVIEW

A. Overview of the Research

Cryptocurrency is a decentralized, digital financial system in which transactions occur on distributed ledgers known as blockchains. Among the thousands of existing cryptocurrencies, bitcoin is the most prominent and foundational, introduced by [2] as a peer-to-peer electronic cash system.
Anomaly detection refers to the process of identifying patterns in data that do not conform to expected behaviour. These anomalies or outliers may signify irregularities such as fraudulent transactions, security breaches or system malfunctions or they may indicate noisy data requiring further pre-processing [3]. In the context of complex systems like financial networks or blockchain environments, anomaly detection plays a vital role in identifying. operational errors, enhancing root cause analysis and supporting real time decision making [4].

Anomaly detection has become increasingly critical across diverse domains, including risk management, cybersecurity, financial fraud detection, healthcare diagnostics, and monitoring AI driven systems for potential safety risks [5]. Recent advances in artificial intelligence which is the capability of machines to imitate intelligence in human behaviour, attained by examining how the human brain thinks and how it learns, decides, and works in solving a specific problem [15] particularly in machine learning and deep learning, have led to more robust and adaptive anomaly detection frameworks. Deep anomaly detection (DAD) leverages neural architectures such as autoencoders, recurrent neural networks (RNNs), and graph neural networks (GNNs) to model complex, high dimensional data and uncover hidden patterns that traditional statistical methods might miss [6]. Deep learning techniques are generally divided into three categories: discriminative learning (supervised learning), generative learning (unsupervised learning), and hybrid learning, which combines elements of both. Each of these paradigms contributes differently to anomaly detection strategies. While discriminative models aim to directly classify inputs, generative models such as autoencoders focus on learning the underlying data distribution, making them particularly useful in unsupervised anomaly detection. Hybrid models, on the other hand, leverage both approaches to enhance performance. As highlighted by [7].

In the cryptocurrency domain where high volatility, decentralized transactions, and pseudonymous behaviour complicate analysis,deep learning based anomaly detection offers distinct advantages. Several studies have proposed deep learning approaches to detect and mitigate anomalies by training models on historical cryptocurrency data [8]. In this research, the comparative analysis of unsupervised models such as K-Means, Isolation Forest, One-Class SVM and deep autoencoders necessitates a structured experimentation framework.These models vary in terms of their assumptions about data distribution, scalability and sensitivity to noise and outliers[3]. bitcoin transactions are publicly recorded on the blockchain and generate high dimensional, time dependent, and graph structured data, the users interface UI serves as a crucial intermediary between complex model outputs and actionable insights. The main objective of the interface is to facilitate interpretability, real time monitoring and user control in identifying and responding to suspicious activity within the bitcoin network [2][9]

B. Related Work

There are many research studies on anomaly detection and these studies use variety of techniques including machine learning and network analysis techniques.

Pocher *et al*, (2023). described anomaly detection in the context of anti-money-laundering (AML) / counter financing of terrorism (CFT) applied graph based and ML forensic analysis to cryptocurrency transactions (including Bitcoin), exploiting network structure and transaction history to detect suspicious flows. This bridges ML methods and real-world compliance needs, showing how detection could support forensic investigations. The paper also compares different algorithms, offering insight into which methods may be more effective for practical AML-style monitoring.

Hussein et al. (2011) applied clustering approaches for anomaly detection, based on the principle that normal behaviours should cluster together while irregular behaviours form distinct groups. In a related study, Smith et al. employed k-means clustering, self-organizing maps, and the expectation-maximization algorithm to build their anomaly detection models.

Asiri and Somasundaram (2025) applied a GCN-based model for detecting illicit transactions, demonstrating stronger accuracy and AUC performance where AUC refers to the Area Under the ROC Curve, a metric that evaluates how well the model distinguishes illicit from legitimate activities when compared with traditional baseline methods. Their work provides a graph-based evaluation framework for early detection, using specific labeled datasets and comparative models. However, they indicate that broader generalization across varying illicit behaviors, adaptive adversarie and real-time operational constraints still requires additional research. The study also underscores the need for larger and more diverse datasets.

Zheng et al. (2017) proposed using a Gephi-generated graph to model address data and employed the Louvain community detection algorithm to infer relationships among users, enabling anonymization while enhancing the traceability of Bitcoin flows for improved future analysis. They describe two common configurations of the Gephi graph: (a) users represented as nodes with transactions as edges, and (b) transactions represented as nodes with users as edges.

Zambre et al. (2013) utilized k-means clustering to identify anomalies in the graph, including incidents such as all in vain theft, Stone Man loss, and large-scale Bitcoin theft. The evaluation examined the relationship between the k-means cost function and the number of clusters, leading to the determination of an optimal clustering approach.

Javarone *et al*, (2020) examined the detection of double-spending attacks by transforming the bitcoin network into a directed acyclic graph, where vertices corresponded to blocks that were created by the miners. The advantage provided by this transformation was that the blocks created by an attacker are not well connected in the graph, and they can be easily detected using specialized clustering approaches, such as spectral clustering, to categorize the graph's vertices into malicious and not malicious.

Hassan *et al*. (2024) introduces an under sampling algorithm (XGBCLUS) specifically tailored for blockchain transaction data. Moreover, the authors integrate explainable AI (XAI) using SHAP (Shapley

Additive Explanations) into tree ensemble classifiers. This allows not only detection of anomalous transactions but also human readable explanations (feature contributions) for why certain transactions are flagged. This dual emphasis on performance and interpretability is a step forward, especially for operational or regulatory contexts where transparency is critical. The study compares ensemble methods versus single classifiers, establishing practical baseline methods.

Siddamsetti, et al. (2023) apply various anomaly detection and deep-learning algorithms including autoencoders, cluster-based outlier detection (CBLOF), isolation forest, and ensemble methods to raw Bitcoin transaction data. The value here lies in exploring unsupervised anomaly detection rather than supervised classification. This is important because many illicit transactions may not have labels; hence unsupervised detection offers a way to flag unknown suspicious patterns. The work demonstrates that even without prior labeling, automated methods can identify outliers that may correspond to fraud offering a baseline for anomaly detection independent of labeled

Perez et al. (2025) This study combines anomaly detection with modern graph based deep learning.It applies Heterogeneous Graph Transformers (HGT) to Bitcoin transaction data, leveraging the relational and heterogeneous nature of blockchain data (addresses, transactions, possibly different transaction types). By doing so, it validates that unsupervised anomaly detection and supervised graph based methods both have merit for fraud detection in cryptocurrency networks. The paper expands the methodological toolkit for blockchain anomaly detection,especially highlighting that graph transformer architectures which can capture complex relational patterns useful beyond traditional GNNs. This contributes to the growing trend of deep, structure-aware detection models

III. METHODOLOGY

In this section we describe data collection and parsing, features extraction and we provide explanations for the unsupervised learning techniques we use.
The cryptocurrency dataset used for this research was obtained from an open access bigquery database. The research employed both users and transaction graphs to investigate anomalies in the bitcoin. The user graph will detect suspicious users while the transaction graph will detect suspicious transactions. Using these two graph representations, we can not only find out both abnormal users and abnormal activities but also check if our methods are consistent in the sense that suspicious transactions should belong to suspicious users.The dataset consists of 1048576 users and transactions**.**

A. Feature Extraction

The research will extract a set of features. In each of the graph representations of the data, The following features will be extracted which includes

For the user graph, the set of features are the followings:

1. In-degree: Number of transactions received by a given user.
2. Out-degree: Number of transactions sent by a given user.
3. Unique in-degree: Number of unique users a given user has received transactions from.
4. Unique out-degree: Number of unique users a given user has sent transactions to.
5. Average in-transaction: Average number of bit coins received per incoming transaction.
6. Average out-transaction: Average number of bit coins sent per outgoing transaction.
7. Number of public keys owned by a given user.
8. Balance: Net number of bit coins retained by user.
9. Clustering coefficient: measure of connectivity amongst neighbours of a given user

For the transaction graph, the set of features are the followings:

1. In-degree: Number of transactions (i.e. nodes) that take money from a given Transaction (a given node).
2. Out-degree: Number of transactions that a given transaction takes money from.
3. Unique in-degree: Number of unique transactions that take money from a given transaction**.**
4. Unique out-degree: Number of unique transactions that a given transaction takes money from.
5. Average in-transaction: Average number of bit coins on each incoming edge to a given transaction.
6. Average out-transaction: Average number of bit coins on each outgoing edge from a given transaction.
7. Number of users a given transaction is associated with.
8. Balance: Net number of bit coins for a given transaction considering all in- and out-going edges from that transaction.
9. Clustering coefficient: measure of connectivity amongst neighbours of a given transaction

B. Unsupervised Learning approaches for Anomaly Detection

Four models were used in this research for robust evaluation which includes Graph convolutional Network, Graph Attention Network Autoencoder, one-class Support Vector Machines and Isolation Forest.Since the data are all unlabelled, the same

dataset will be used to train and testing on each of the developed models.
Unsupervised learning, particularly in graph based models such as Graph Neural Networks (GNNs), evaluating the performance becomes challenging. To address this challenge, a set of evaluation metrics will be used to assess the quality and the effectiveness of anomaly detection.

IV. EXPERIMENTATION

The dataset consists of both users and transaction dataset. The datasets were split into two parts: 70 percent for training and 30 percent for testing. The research trained and test on four m/odels: graph autoencoders (GAE) using Graph Convolutional Networks (GCNs), attention based autoencoders (GAT-AE) using Graph Attention Networks (GATs) and classical anomaly detection models such as One-Class SVM and Isolation Forests. For GCN GAE and GAT-AE models, node features and edge indices were used to encode node embedding through two layers architecture. These embedding were optimized to reconstruct the original graph structure using link prediction loss. Each GNN model was trained for 100 epochs using the Adam optimizer, with a learning rate of 0.001 and a batch size determined by the system configuration. Losses were logged at regular intervals to monitor training progress. A grid search was conducted on the GNN models to analyze its sensitivity to key hyperparameters. The search focused on hidden dim, attention heads, and dropout. The final configuration of `hidden dim= 32, heads= 4, dropout= 0.6 was found to be effective and used for the main architecture search. The high performance across the grid suggests that the gnn architecture is robust and not overly sensitive to minor variations in these parameters. For the One-Class SVM, node features were scaled using Standard Scalar, and a random sample of up to 200,000 nodes was used to train and test the model with an RBF kernel and nu=0.1. Anomaly scores were computed by evaluating the model's decision function across the full dataset. In the case of the Isolation Forest, the research applied the model with a contamination rate of 0.1 to detect outliers based on node distributions.

V. Performance Evaluation Metrics

A. *Silhouette Score*

Silhouette Score is an unsupervised learning metric that measures how well separated the identified clusters of nodes are in the embedding space. It measures the similarity of a data point belonging to a specific cluster in relation to the rest of the clusters[18]. In this context, this research derives binary labels (anomalous vs. normal) based on the anomaly score percentile. A high silhouette score indicates that the model produces distinct, well defined clusters for normal and anomalous nodes. This score ranges from -1 to 1, where values close to 1 indicate well clustered points, values near 0 suggest overlapping clusters, and negative values signal potential misclassification [31]

B. *t-SNE: Visualizing High Dimensional Embedding Spaces*

While quantitative metrics like the Silhouette Score and mDE provide numerical insights, t-distributed Stochastic Neighbour Embedding (t-SNE) offers a powerful visual inspection tool for understanding the structure of learned embeddings in high dimensional spaces.t-SNE reduces high dimensional data (such as node embeddings) to two or three dimensions while preserving local neighbourhood relationships. It models pair wise similarities using a probabilistic framework and optimizes the low dimensional embedding to reflect those similarities as accurately as possible. The result is a visual map where similar points are close together, and dissimilar points are far apart.
In the context of anomaly detection:

- Normal nodes tend to form dense clusters.
- Anomalous nodes appear as outliers or form distinct small clusters.
- When overlaid with colour coded anomaly scores or cluster labels, t-SNE plots can provide intuitive confirmation of a model's effectiveness.

t-SNE serves as an essential interpretability and debugging tool, helping researchers assess whether the model's embedding space is meaningfully structured.

C. *Mean Dual Evaluation (mDE):*

Unlike clustering-based metrics, the Mean Dual Evaluation (mDE) is tailored specifically for unsupervised anomaly detection in graphs, particularly when using models like autoencoders or graph convolutional networks designed to reconstruct the input data.
The "dual" in mDE refers to the simultaneous evaluation of two critical components:

- Structural reconstruction loss, such as the error in reconstructing the adjacency matrix.
- Attribute reconstruction loss, which measures the fidelity of reconstructed node features (if available).

The mDE metric is generally computed as the average or weighted combination of these two losses. Its formulation may vary by implementation, but a common form is:

$$C1 = \frac{A_N \cap topANtrasactionaloutliers}{A_N} \qquad Eqn\ 1$$

$$C2 = \frac{B_M \cap topBMuseroutliers}{B_M} \qquad Eqn\ 2$$

$$mDE = \frac{C1 + C2}{2} \qquad Eqn\ 3$$

Note that *mDE* ∈[0, 1] and the bigger it is, the more accurate.
A_N - the set of transactions corresponding to the top N node outliers and
B_M - the set of users corresponding to the top M transaction outliers defined above.

V. Results and Discussion

The figures below show result of applying t-SNE (t-Distributed Stochastic Neighbor Embedding) to high-dimensional bitcoin transactions and users dataset, and then coloring the points based on K-Means clustering with 2 clusters. t-SNE reduces high-dimensional data into 2 dimensions that can be visualized. Each dot in the plot represents one Bitcoin transaction. t-SNE tries to place similar transactions and users closer together and also spreads out dissimilar ones.

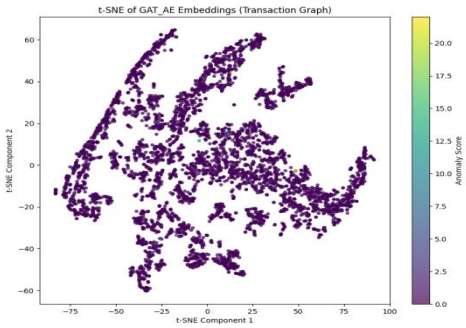

Figure1:t-SNE GAT-AE Embedding Transaction Graph

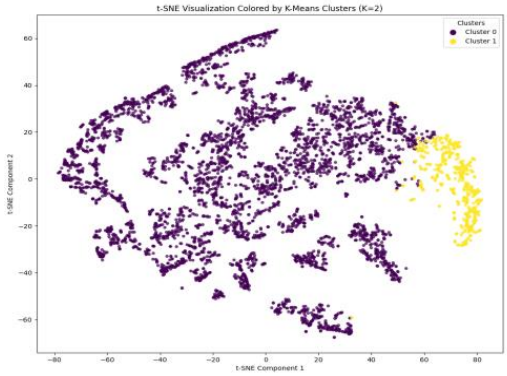

Figure 2: t-SNE GAT-AE K Means Cluster Transaction Graph

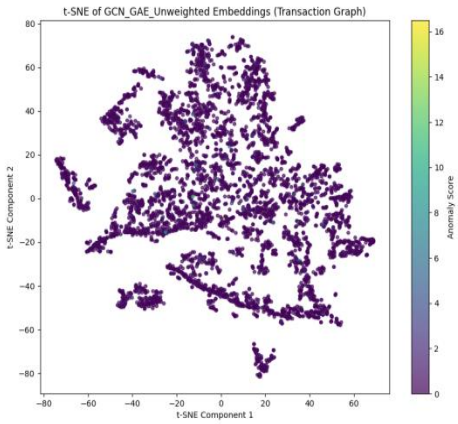

Figure3: t-SNE GCN-GAE Transaction Graph Embedding

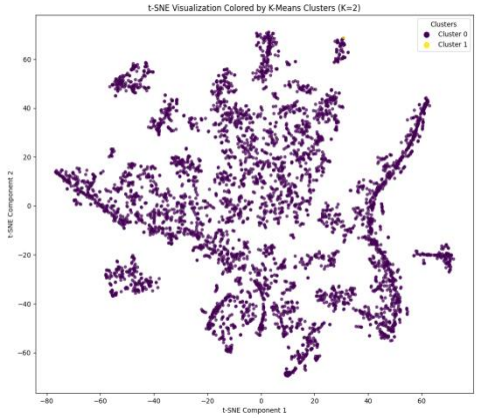

Figure 4: t-SNE GCN Transaction Graph Colored by the k-Means Clusters.

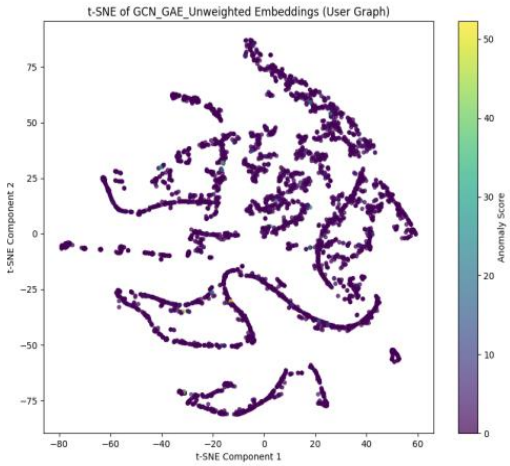

Figure 5: t-SNE GCN-GAE Embeddings User Graph

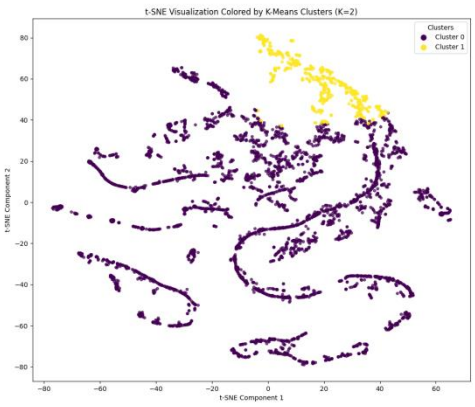

Figure 6: t-SNE GCN-GAE Kmeans Cluster User Graph

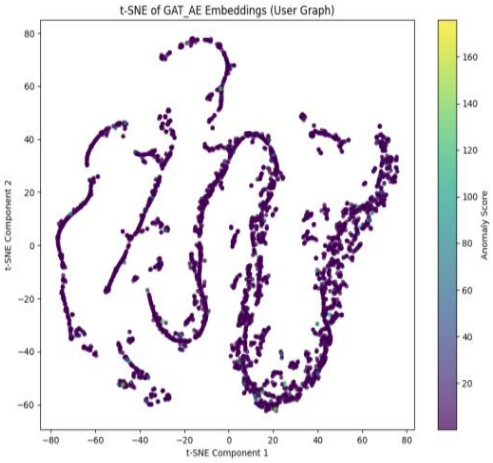

Figure 7: t-SNE GAT-AE Embedding User Graph

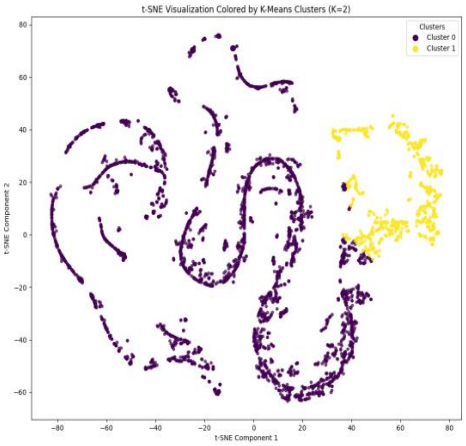

Figure 8: t-SNE GAT-AE K-Means Cluster User Graph

When evaluated on cross graph consistency, a clear performance hierarchy emerged from the mDE scores. The GAT AE was the top performer with a score of 0.251, followed closely by the GCN GAE at 0.145. The classical models were less effective, with the One-Class SVM scoring 0.043 and the Isolation Forest yielding the lowest score of 0.024.

Table 1: Results from train and test for transaction

Model	Silhouette Score (Transaction)
GCN AE	0.691
GAT AE	0.673
One Class SVM	0.571
Isolation Forest	0.432

Table 2: Results obtained after training and testing for User

Model	Silhouette Score (User)
GCN AE	0.922
GAT AE	0.754
One Class SVM	0.442
Isolation Forest	0.424

Table 3: mDE Result (Cross Graph Consistency Metric)

Model	Result
GAT AE	0.251
GCN AE	0.145
One Class Svm	0.043
Isolation Forest	0.024

VI. CONCLUSION

This research conducted a comprehensive evaluation of unsupervised anomaly detection on the bitcoin network, comparing the performance of graph based deep learning models against classical machine learning algorithms on both user and transaction graphs. The primary finding of this research is the superiority of Graph Neural Networks in identifying contextual and structural anomalies. While classical models such as the One-Class SVM proved competent at detecting nodes that were statistical outliers based on their intrinsic features, the GNNs models consistently demonstrated a more sophisticated capability.This research successfully demonstrates that graph based deep learning models represent a significant advancement in the field of unsupervised anomaly detection on the cryptocurrency network.

References

[1] Sarwar, M. I., Nisar, K., & Khan, A. (2019, September). Blockchain-from cryptocurrency to vertical industries-a deep shift. In *2019 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)* (pp. 1-4). IEEE.

[2] Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, *4*(2), 15.

[3] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM computing surveys (CSUR)*, *41*(3), 1-58.

[4] Goldstein, M., & Uchida, S. (2016). A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. *PloS one*, *11*(4), e0152173.

[5] *Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31*.

[6] Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. *arXiv preprint arXiv:1901.03407*

[7] Mounnan, O., Manad, O., El Mouatasim, A., Boubchir, L., & Daachi, B. (2023). Deep Speech Recognition System Based on Auto Encoder-GAN for Biometric Access Control. *International Journal of Advanced Computer Science & Applications*, *14*(11).

[8] *Hassan, M. U., Rehmani, M. H., & Chen, J. (2022). Anomaly detection in blockchain networks: A comprehensive survey. IEEE Communications Surveys & Tutorials. 25(1). 289-318*

[9] Zhou, B., Liu, S., Hooi, B., Cheng, X., & Ye, J. (2019, August). Beatgan: Anomalous rhythm detection using adversarially generated time series. In *IJCAI* (Vol. 2019, pp. 4433-4439).

[10] *Leskovec, J., Kleinberg, J., & Faloutsos, C. (2007). Graph evolution: Densification and shrinking diameters. ACM transactions on Knowledge Discovery from Data (TKDD), 1(1), 2-es.*

[11] *Issa, H. (2011). Application of anomaly detection techniques to identify fraudulent refunds. SSRN Electronic Journal.*

[12] *Breunig, M. M., Kriegel, H. P., Ng, R. T., & Sander, J. (2000, May). LOF: identifying density-based local outliers. In Proceedings of the 2000 ACM SIGMOD international conference on Management of data (pp. 93-104).*

[13] *Zheng, B., Zhu, L., Shen, M., Du, X., Yang, J., Gao, F., & Yin, S. (2017, December). Malicious bitcoin transaction tracing using incidence relation clustering. In International Conference on Mobile Networks and Management (pp. 313-323). Cham: Springer International Publishing.*

[14] *Zambre, D., & Shah, A. (2013). Analysis of bitcoin network dataset for fraud. unpublished Report, 27, 2013.*

[15] *Abhulimen, O., & Ogunti, E. (2021). Facial age estimation using deep learning: A review. methods, 8(5).*

[16] *Javarone, M. A., & Wright, C. S. (2018). Modeling a double-spending detection system for the bitcoin network. arXiv preprint arXiv:1809.07678.*

[17] *Biryukov, A., & Tikhomirov, S. (2019, April). Transaction clustering using network traffic analysis for bitcoin and derived blockchains. In IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 204-209). IEEE.*

[18] *Cholevas, C., Angeli, E., Sereti, Z., Mavrikos, E., & Tsekouras, G. E. (2024). Anomaly detection in blockchain networks using unsupervised learning: A survey. Algorithms. 17(5). 201.*

[19] Kipf, T. N. (2016). Welling M (2016a) Semi-supervised classification with graph convolutional networks. *arXiv preprint arXiv:1609.02907*.

[20] *Leiserson, C. E. (2019). Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics. arXiv preprint arXiv:1908.02591.*

[21] Pham, T., & Lee, S. (2016). Anomaly detection in the bitcoin system-a network perspective. *arXiv preprint arXiv:1611.03942*.

[22] *Pourhabibi, T., Ong, K. L., Kam, B. H., & Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. Decision Support Systems, 133, 113303.*

[23] *Veličković, P., Cucurull, G., Casanova, A., Romero, A., Lio, P., & Bengio, Y. (2017). Graph attention networks. arXiv preprint arXiv:1710.10903.*

[24] *Odufisan, O. I., Abhulimen, O. V., & Ogunti, E. O. (2025). Harnessing Artificial Intelligence and Machine Learning for Fraud Detection and Prevention in Nigeria. Journal of Economic Criminology, 100127.*

[25] *Asiri, A., & Somasundaram, K. (2025). Graph convolution network for fraud detection in bitcoin transactions. Scientific Reports, 15(1), 11076.*

[26] *Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M. Z., & Ferretti, S. (2023). Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. Electronic Markets, 33(1), 37.*

[27] *Hasan, M., Rahman, M. S., Janicke, H., & Sarker, I. H. (2024). Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis. Blockchain: Research and Applications, 5(3), 100207.*

[28] *Siddamsetti, S., & Srivenkatesh, M. (2024). Deep blockchain approach for anomaly detection in the bitcoin network. International Journal of Intelligent Systems and Applications in Engineering, 12(1), 581-595.*

[29] *Pérez-Cano, V., & Jurado, F. (2025). Fraud detection in cryptocurrency networks—An exploration using anomaly detection and heterogeneous graph transformers. Future Internet, 17(1), 44.*

[30] *López-Sorribes, S., Rius-Torrentó, J., & Solsona-Tehàs, F. (2023). A bibliometric review of the evolution of blockchatechnologies. Sensors, 23(6), 3167.*

[31] Shutaywi, M., and Kachouie, N. N. (2021). Silhouette analysis for performance evaluation in machine learning with applications to clustering. *Entropy*, *23*(6), 759.