

BLOCKCHAIN FORENSICS: TRACKING ILLICIT CRYPTOCURRENCY TRANSACTIONS USING AI

2505249 – Sanjay kumar Unkili

**UNIVERSITY OF WALES TRINITY SAINT DAVID – Wales Institute of Science and
Arts – School of Applied Computing**

Table of Contents

1. INTRODUCTION	3
1.1 Context and Background.....	3
1.2 Research Problem.....	3
1.3 Research Aim and Objectives	4
1.4 Significance of the Research	5
2. LITERATURE REVIEW	6
2.1 Blockchain Forensics Techniques.....	6
2.2 Machine Learning in Crypto Crime Detection.....	6
2.3 Graph-Based Approaches (GNNs).....	7
2.4 Theoretical & Technical Frameworks.....	8
2.5 Research Gap.....	9
2.6 Relation to the Study	9
2.7 Literature Summary.....	10
3. RESEARCH DESIGN & METHODOLOGY	11
3.1 Research Design.....	11
3.2 Methods.....	11
3.3 Materials.....	12
4. EXPECTED OUTCOMES	13
5. TIMELINE.....	13
Reference List	15

1. INTRODUCTION

1.1 Context and Background

Cybersecurity and digital finance Blockchain Technology has become a revolutionary innovation, which allows recording transactions in a decentralized, transparent, and immutable manner. Meanwhile, Artificial Intelligence is also becoming a part of security systems to process large amounts of transactional data and identify anomalies. The most recent rise in cryptocurrencies, including Bitcoin and Ethereum, has also caused remarkable changes in the adoption of blockchains, with the global blockchain market already estimated to be worth 12.3 billion in 2023 and is expected to attain 289.2 billion by 2030 [1].

Nevertheless, this growth has also helped the emergence of crypto-enabled cybercrime. Criminal activities such as ransomware, darknet market transactions, and money laundering have become common. To give an example, in 2025, ransomware attackers alone were paid more than 820 million USD in cryptocurrency and volume of illicit cryptocurrency around the world amounted to 158 billion USD, which demonstrates the amount of financial crime in blockchain ecosystems [2,3]. Such trends point to the way cybercriminals are taking advantage of the pseudonymous character of blockchain transactions to mask identities and escape detection.

Blockchain systems are transparent by nature, and all the transactions are publicly recorded, but with no direct identity association, it can be extremely difficult to investigate any particular transaction. This has led to the emergence of blockchain forensics, a specialised field focused on analysing transaction flows, wallet interactions, and behavioural patterns to identify illicit activities [4].

The new developments are also tracked by usage of advanced techniques of analysis. The application of machine learning and artificial intelligence algorithms is increasingly being applied to financial crime detection, but graph-based analytics may be employed to model the connection among the transactions. Moreover, heightened regulatory requirements, particularly, the Anti-Money laundering (AML) and Know Your Customer (KYC) regimes are also adding to the fact that they require more powerful forensic solutions. Together, these technological and regulatory trends highlight the imperative urgency of smart and data-driven approaches to enhance blockchain forensic research.

1.2 Research Problem

Although blockchain analytics have evolved, there is a difficulty in detecting illegal transactions of cryptocurrencies. The existing blockchain forensic tools do not detect malicious

activities due to the continually changing and sophisticated obfuscation techniques, such as mixing services, chain hopping, and privacy-enhancing protocols. Such techniques take advantage of the fact that the Blockchain Technology is inherently pseudonymous, with wallet addresses not necessarily associated with the real-life identity, which is hard to attribute.

The most crucial weakness is the dire class imbalance present in the transaction datasets where the illicit transactions usually make up less than 1–2% of all activity [5]. This bias negatively affects the performance of the classical machine learning models, which are biased to the majority (licit) category. In addition, due to the scarcity of quality labelled data, supervised learning practices are limited, which also limits the power of models to generalise and be strong.

Although they are useful, traditional machine learning methods do not reflect the intricate relational nature of blockchain networks. Transaction interdependency: Higher-level, interdependent models that fail to take into account interdependencies among transactions will easily produce suboptimal results. The techniques such as address clustering which are heuristic-based are also more prone to inaccuracy and are easily compromised by adversaries. Scalability is another issue because blockchain networks produce large amounts of data, and their analysis needs to be computationally efficient but precise analytical methods. These restrictions underline the necessity of the further development of the methods of illegal cryptocurrency transactions detection that should be more advanced, graph-aware, and scalable.

1.3 Research Aim and Objectives

Aim

The main aim of the work is to develop and test sophisticated machine learning and graph-based models to identify illegal cryptocurrency transactions with the highest accuracy, enhance blockchain forensic and overcome the limitations of current analytical and detection methods.

Objectives

- To critically examine available methods of blockchain forensics and determine its shortcomings in detecting criminal cryptocurrency transactions in changing cybercrime contexts.
- To preprocess and explore the Elliptic Bitcoin Dataset, to deal with class imbalance, feature relevance, and data quality problems to prepare the model.
- To apply and test a baseline Random Forest model to predict licit and illicit transactions of cryptocurrency transactions using structured features of transactions.

- To build and optimise an XGBoost model to enhance the performance of the classification, it is necessary to pay attention to the imbalanced data and the improvement of the level of prediction.
- To develop and deploy a Graph Neural Network model with transaction relationships, and compare performance to baseline models with standard evaluation metrics.

1.4 Significance of the Research

The research is topical as it is one of the answers to the growing problem of detecting illegal activity within the cryptocurrency sector that will directly assist the law enforcement officers in tracking financial crimes, such as money laundering and ransomware payments. The study will use advanced Artificial Intelligence and graph-based models, which can help improve the accuracy and efficiency of fraud detection systems, and minimize the constraints of the traditional methods. This can be used to improve the existing Cybersecurity systems as suspicious patterns of transactions can be detected beforehand.

In practice, the results can be applied in financial institutions and cryptocurrency exchanges to improve their adherence to the Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations. These insights can also be used by regulatory bodies to come up with stronger monitoring mechanisms. This has an intellectual contribution to the advancement of blockchain forensics, in which this study integrates machine learning with graph analytics to offer a novel and scalable framework of detecting illicit dealings in cryptocurrencies.

2. LITERATURE REVIEW

2.1 Blockchain Forensics Techniques

The main techniques used in blockchain forensics are tracing of transactions, clustering of addresses and heuristic analysis to detect illegal transactions. Transaction tracing has taken advantage of the transparency of the Blockchain Technology to trace the flow of money among wallets to enable the investigators to trace the monetary trail in order to reverse the flow of money. Address clustering also increases this process by clustering together multiple wallets address that are likely to be used by the same entity. An example done in research, suggested the BACH tool, which integrates several heuristics to enhance the accuracy of clustering and visualisation of relationships using a graph [6]. They find that multi-heuristic methods are more effective in producing more comprehensive clusters compared to single-heuristic methods.

Nevertheless, these methods have major drawbacks. Heuristic approaches are usually based on assumptions regarding transaction behaviour and so, can be circumvented by evasion strategies such as address reuse avoidance and mixing services. Research indicate that the absence of trustworthy labelled data and the development of privacy-enhancing techs lower the accuracy of clustering outcomes as a forensic piece of evidence [7]. Also, scalability is an issue; to analyse big data in blockchain, it is necessary to apply sophisticated methods of computing. Research proves that hundreds of millions of transactions require distributed systems to be processed effectively [8]. In general, these methods are fundamental but not very accurate and prone to obfuscation, which requires more sophisticated, data-driven methods.

2.2 Machine Learning in Crypto Crime Detection

The use of machine learning methods has taken the centre stage in the determination of illegitimate cryptocurrency transactions in the Blockchain Technology systems. Classical supervised learning algorithms like the Random Forest, Support Vector Machines (SVM) and the Logistic Regression have been extensively used in classification. Research studies like Studies illustrate that these models do provide sufficient potential to differentiate between legitimate and fraudulent transactions based on structured features [9]. In the same way, research demonstrate that ensemble and tree-based approaches are better at classifying data when hyperparameter optimization is employed [10]. They are computationally efficient and interpretable and so can be used in the implementation of a baseline.

Nevertheless, there are significant shortcomings of these traditional models. They consider transactions as independent data points, thus disregarding the graph nature of blockchain networks. This causes a loss of relational information among transactions which is important

in the identification of coordinated illicit behaviour. They also have a problem of extreme class imbalance, in which illegal transactions constitute a tiny subset of the data, and frequently, prediction is biased towards the majority class.

In order to address these shortcomings, a more sophisticated models like Extreme Gradient Boosting (XGBoost) and deep learning models have been proposed. The article by presented a machine learning framework (VTAC), which has an accuracy of 97.5% based on XGBoost, which is higher than the traditional models [10]. Similarly, a study indicated that XGBoost was very effective with ransomware related Bitcoins as it was able to identify the patterns with a high accuracy of 99.08. XGBoost also offers feature importance inferences, which allow more interpretability of influential attributes of transactions [11].

The predictive performance of Deep learning models and ensembles can further be enhanced by the capture of non-linear relationships in transaction data. Indicatively, research illustrate that refined boosting algorithms like LightGBM delivered higher accuracies of more than 99 percent, surpassing various conventional classifiers [12].

In spite of these advances, there is still a gaping hole. The majority of machine learning models such as the XGBoost and deep learning approaches are mostly based on tabular transaction features and do not consider the relational dependencies among transactions. As a result, they lack sufficient powers to detect complex laundering schemes that traverse numerous related addresses. This highlights the importance of the graph-based models, e.g., Graph Neural Networks, as an addition to the current models and to improve blockchain forensic analysis.

2.3 Graph-Based Approaches (GNNs)

Graph-based approaches, particularly, Graph Neural Networks (GNNs), have emerged as one of the most powerful paradigms to investigate illegal cryptocurrency transactions within the systems of Blockchain Technology. Unlike traditional machine learning models, GNNs directly correspond to graphical data of blockchain, with nodes being transactions and edges being transaction flows. This makes it easier to obtain complex relational dependences, which are crucial in identifying even the sophisticated money laundering systems such as layering, fan-out and mix-ups of transactions.

Recent studies have shown the applicability of GNNs in this field. As shown by a work, even complex GNN models, like Graph Convolutional Networks (GCNs) and Graph Attention Networks (GATs), significantly positively affect the quality of classification, compared to traditional approaches [12]. Similarly, study also reveal that GNNs outperform other models like the Random Forest and XGBoost since they employ structural and topological features of

blockchain networks [13]. Additionally, a heterogeneous graph framework integrates the multi-dimensional data on transactions, which enhances its interpretation ability and enables the detection of the fraud on a broader level [14].

Despite these advantages, there are various obstacles which limit the extensive use of GNNs. As study point out, extreme class imbalance, i.e. illegal transactions being below 2 percent of the dataset also affects the stability and reliability of models substantially [14]. Furthermore, GNNs are difficult to train on large blockchain graphs because it consumes a lot of memory and is computationally complex. Other problems that may render them challenging to apply in real-life forensic investigations are structural sparsity, label noise and lack of explainability. Therefore, although GNNs are a promising and fast-developing field of research, their application is still scarce. In order to fully realise the potential of using graph-based learning to scalable and reliable blockchain forensic analysis, these issues should be addressed.

2.4 Theoretical & Technical Frameworks

The research relies on several theoretical and technical frameworks, which are inter-related, and capable of assisting blockchain forensics and detection of illicit transactions. First of all, blockchain data is modelled with the help of graph theory. Transactions involving cryptocurrencies inherently create graph-like networks, with the nodes modelling transactions and edges modelling fund flows. This representation enables the investigation of the connectivity, centrality and patterns of transactions which are crucial in identifying illicit behaviour. Graphical representations are crucial since the conventional tabular methods do not reflect such relational dependencies [13].

Secondly, classification works in blockchain forensics are based on supervised learning. The labelled datasets (licit vs illicit transactions) are used to train models to learn the discriminative patterns. However, they are very reliant on labelled data, which is usually scarce in the real blockchain environment, thus constraining the possibility of generalisation [15].

Building upon this, ensemble learning enhances predictive potential through a combination of a group of models to reduce variance and enhance robustness. Ensemble-based graph learning models are based on the idea that a large range of structural patterns of blockchain data can be modelled by combining the different Graph Neural Networks (e.g., GCN, GAT, GIN), leading to improved detection accuracy and reduced false positives [15].

Lastly, deep learning, specifically, Graph Neural Networks, is essential in the representation of features of nodes and topological connections. GNNs make use of message-passing schemes

to calculate the information of the neighbouring nodes and, hence, determine the intricate patterns of transactions that cannot be detected with the aid of the traditional models.

These frameworks are effective, but they also have issues such as: they depend on labelled data, are computationally and scalability complex. The combination of these methods, especially the combination of supervised, ensemble, and graph-based deep learning can serve as a comprehensive framework of developing blockchain forensic analysis.

2.5 Research Gap

Recent research has made a big step in the area of blockchain forensics, establishing enhanced methods of analysis to identify unlawful transactions in cryptocurrency. The methods could be improved by incorporating multiple heuristics, which improved the identification of wallet entities due to heuristic-based methods [9]. Similarly, it has been demonstrated that machine learning-based methods have high classification performance; Studies have a high detection accuracy on the use of XGBoost to identify suspicious patterns, which highlights the value of ensemble learning [11]. In addition, the latest advances in graph approaches, namely Graph Neural Networks, have helped to model intricate connection among transactions which have significantly enhanced detection in highly connected blockchain environments.

In spite of these contributions, there are still a number of critical gaps. The majority of traditional and machine learning methods have a strong dependence on tabular features and do not completely reflect the relationship and time dynamics of blockchain transactions. Although GNN-based approaches can overcome this drawback, research, like Lawal et al., demonstrates issues associated with class imbalance, scalability, and model interpretability. Moreover, little research has been done to combine ensemble learning with graph-based deep learning to utilize both feature-based and structural information. Hence, there is a need to have a holistic, hybrid solution to these shortcomings in order to enhance the effectiveness and strength of blockchain forensic analysis.

2.6 Relation to the Study

This work is based on the current research in blockchain forensics and incorporates and expands previous contributions to the field of machine learning and graph-based analytics. Although past research has shown the effectiveness of models like Random Forest, XGBoost, and Graph Neural Network separately, they usually consider them separately. The study contributes to the domain by presenting a hybrid approach to ensemble learning and graph-based deep learning that would utilize both feature-level and relational information in the Blockchain Technology systems.

This is in contrast to previous literature, where researchers either seek to improve the accuracy of classification or to model the relationship between transactions, but this work seeks to integrate both to promote better detection of transactions in high imbalanced data sets. Further, the research has offered a comprehensive description of the evaluation framework by systematically comparing the baseline, advanced, and graph-based models with the same dataset. This method brings fresh knowledge about the effectiveness of the models, their scaling, and applicability, and add a more sound and practical solution to real-life blockchain forensic investigations.

2.7 Literature Summary

In the review of literature, the authors note that heuristic and machine learning models and graph-based approaches improve blockchain forensics greatly. Clustering, a heuristic technique has been used to improve on tracking transactions but it is less precise and it is prone to evasion techniques. The classical machine learning models such as the Random Forest and the Logistic Regression are the ones that offer a baseline level of classification performance yet do not reflect the relationship of the Blockchain Technology data and cannot deal with the unbalanced classes. More advanced models like XGBoost and boosting methods have better accuracy and feature importances, but are still mainly based on tabular data.

More recently, Graph Neural Networks have also been developed as useful in modelling transaction relationships and have greatly improved the ability to detect complex laundering patterns. Nevertheless, issues of difficulty in computation, scalability, imbalance in classes, and lack of interpretability remain. As a whole, the literature shows that there is an evident gap in the combination of feature-based and graph-based methods, and hybrid, scalable, and robust solutions are required to enhance the detection of illicit transactions.

3. RESEARCH DESIGN & METHODOLOGY

3.1 Research Design

This work includes a Design Science Research (DSR) integrated with experimental research to solve the issue of identifying illegal cryptocurrency transactions. Design Science will suit because the study is aimed at creating new artefacts, i.e., machine learning and graph-based models, to enhance blockchain forensic analysis. The analysis will entail the design, execution and optimization of models like Random Forest, XGBoost and Graph Neural Networks to help to increase detection levels in Blockchain Technology systems.

The experimental component will be required to figure out the performance of these models in real-life data in a systematic manner. The Elliptic dataset will be controlled and experimented and models will be trained and tested based on the conventional evaluation metrics, such as accuracy, precision, recall, F1-score, and ROC-AUC. This allows the objective comparison and validation of results.

A combination of both methods is supported by previous studies. To illustrate the point, studies applied an experimental machine learning model to assess the performance of the model to identify illicit transactions and proved that structured experimentation is effective in validating predictive models [11]. Thus, the combination of design and experimental approaches is a guarantee that will allow developing innovative solutions and performing strict performance evaluation.

3.2 Methods

The research follows a quantitative data-driven approach, as it is aimed at analysing the structured transaction data, in order to identify the illicit cryptocurrency transactions. The quantitative method fits well since it allows objective numerical measurement of model performance with the help of statistical and computational methods. The paper adheres to an experimental research approach, in which a series of machine learning and graph-based models are applied and tested on a real-life dataset. This methodology guarantees the reproducibility and enables one to conduct systematic contrast of various methods used on the data on the Blockchain Technology.

The suggested system architecture comprises of a number of important steps. Firstly, the Elliptic Bitcoin Dataset is pre-processed with the processing of missing values, the labelling of transactions (licit and illicit), and feature normalisation. This is done to guarantee quality of data and also ready the dataset to be used in training the model.

The analysis of features then follows the exploratory analysis of data to learn about the feature distributions, identify the presence of imbalance in the classes, and find the attributes that are likely to have an impact on the classification of a transaction.

This is followed by the construction of graphs with NetworkX, with nodes defined as transactions, and edges defined as the flow of money. This allows the relational dependency modelling between transactions, which is very important in identifying intricate illicit patterns. There are three approaches within the model training phase. The model used as a baseline is a Random Forest classifier, which is robust and interpretable. The main model is XGBoost due to its better performance in working with structured and unbalanced data. Furthermore, a Graph Neural Network (GNN) model is trained to learn both topological and relational information in the transaction graph, which offers more information on the transaction behaviour.

Lastly, the models are tested based on general performance metrics, such as accuracy, precision, recall, F1-score and ROC-AUC. These measures will give a complete evaluation of classification effectiveness, especially at the imbalanced datasets to guarantee that it can be effectively compared to other models and that the proposed method is working.

3.3 Materials

The present study uses Elliptic Bitcoin Dataset (<https://www.kaggle.com/datasets/ellipticco/elliptic-data-set>), one of the popular real-life datasets to examine the cryptocurrency transactions within the systems of the Blockchain Technology. The data contains the labelled transactions (licit and illicit) and time and structural properties and is highly adapted to the supervised and graph-based learning. Its wide application in the previous scholarly studies predetermines reliability, comparability, and validity of outcomes and enables sound experimental analysis.

Ethically, personally identifiable information is not present in the dataset as a blockchain transaction is pseudonymous by default. This guarantees adherence to data protection principles as well as the reduction of privacy risks. Also, the study will comply with responsible Artificial Intelligence practices, including providing transparency in model creation, preventing the amplification of bias, and concentrating on legal uses of AI, including fraud prevention and financial crime.

It will be implemented using Python as the main programming language because it has a large ecosystem of data analysis and machine learning. Notable libraries are Scikit-learn, which is used to create baseline models, XGBoost, which is used to create high-performance ensemble learning, PyTorch or TensorFlow, which is used to create deep learning models and Graph

Neural Networks, and NetworkX, which is used to create graph models and analyse graphs. On the hardware side, Google Colab will be used to deliver accessible cloud-based computational resources, such as GPU acceleration to train computationally-intensive GNN models.

4. EXPECTED OUTCOMES

The expected outcome of the work is that the advanced models will outperform the baseline approach in detecting illicit cryptocurrency transactions. In particular, XGBoost should classify better than Random Forest since it is more efficient in dealing with complex feature interactions and imbalanced data. Moreover, it is expected that the Graph Neural Network (GNN) model should be the most performance-optimal solution since it will be able to consider the attributes of transactions, as well as the relational structure of blockchain networks. This is especially critical in detecting advanced laundering schemes that might not be apparent using feature-based models.

It is hoped that the findings will help to build more efficient blockchain forensic tools that will allow investigators to better trace suspicious cryptocurrency flows. With practical implications, the study might assist in more robust financial institutions, crypto exchanges, and regulatory agency fraud detection systems related to Anti-Money Laundering (AML) monitoring.

Nonetheless, a number of restrictions are expected. The Elliptic data can limit generalisability as it is a particular blockchain setting and has few labelled illicit cases. Moreover, the cost of training GNNs can be high. Moreover, concept drift and evolving criminal tactics in blockchain ecosystems can also affect model performance.

5. TIMELINE

<i>Activity</i>	<i>Week 1–2</i>	<i>Week 3–4</i>	<i>Week 5–6</i>	<i>Week 7–8</i>	<i>Week 9–10</i>	<i>Week 11–12</i>
Define research scope and refine problem statement	✓					
Conduct initial literature search (databases, journals)	✓	✓				
Critically review blockchain forensic techniques		✓				
Analyse machine learning and GNN literature		✓	✓			
Finalise research gap and objectives		✓				

Acquire and understand Elliptic dataset structure			✓			
Perform data cleaning and preprocessing			✓	✓		
Conduct exploratory data analysis and feature selection			✓	✓		
Construct transaction graph using NetworkX				✓		
Implement Random Forest baseline model				✓		
Develop and tune XGBoost model				✓	✓	
Design and implement Graph Neural Network model					✓	
Perform model training and validation					✓	
Evaluate models using performance metrics					✓	✓
Comparative analysis of model results						✓
Draft methodology and results chapters						✓
Final proofreading, formatting, and submission preparation						✓

Reference List

- [1] “Report: Chainalysis Business Breakdown & Founding Story | Contrary Research,” *Contrary.com*, 2014. <https://research.contrary.com/company/chainalysis>
- [2] C. Team, “Crypto Ransomware: 2026 Crypto Crime Report,” Chainalysis, Feb. 26, 2026. <https://www.chainalysis.com/blog/crypto-ransomware-2026/>
- [3] D. Kuhn, “Illicit actors capture nearly 3% of crypto liquidity in 2025: TRM,” The Block, Jan. 28, 2026. <https://www.theblock.co/post/387453/illicit-actors-capture-nearly-3-of-crypto-liquidity-in-2025-trm> (accessed Apr. 29, 2026).
- [4] C. Team, “Crypto Ransomware: 2026 Crypto Crime Report,” Chainalysis, Feb. 26, 2026. <https://www.chainalysis.com/blog/crypto-ransomware-2026/>
- [5] Paweł Rejkowicz, “Blockchain Analysis in Action: Real-Life Use Cases and Insights,” ULAM LABS, Dec. 03, 2024. <https://www.ulam.io/blog/blockchain-analysis-in-action-real-life-use-cases-and-insights#>
- [6] A. A. Compagnino et al., “An Introduction to Machine Learning Methods for Fraud Detection,” *Applied Sciences*, vol. 15, no. 21, p. 11787, Nov. 2025, doi: <https://doi.org/10.3390/app152111787>.
- [7] M. Caringella, F. Violante, F. De Lucci, S. Galantucci, and M. Costantini, “BACH: A Tool for Analyzing Blockchain Transactions Using Address Clustering Heuristics,” *Information*, vol. 15, no. 10, p. 589, Sep. 2024, doi: <https://doi.org/10.3390/info15100589>.
- [8] Y. Gong, K. P. Chow, and S. M. Yiu, “Improved Bitcoin simulation model and address heuristic method,” *Forensic Science International: Digital Investigation*, vol. 53, p. 301935, Jul. 2025, doi: <https://doi.org/10.1016/j.fsidi.2025.301935>.
- [9] B. Kılıç, C. Özturan, and A. Sen, “Parallel analysis of Ethereum blockchain transaction data using cluster computing,” *Cluster Computing*, Jan. 2022, doi: <https://doi.org/10.1007/s10586-021-03511-0>.
- [10] “IEEE Xplore Full-Text PDF”:, Ieee.org, 2026. <https://ieeexplore.ieee.org/iel8/6287639/6514899/10658980.pdf> (accessed Apr. 29, 2026).

- [11] Suleiman Ali Alsaif, “Machine Learning-Based Ransomware Classification of Bitcoin Transactions,” *Applied Computational Intelligence and Soft Computing*, vol. 2023, pp. 1–10, Jan. 2023, doi: <https://doi.org/10.1155/2023/6274260>.
- [12] “IEEE Xplore Full-Text PDF”:, *Ieee.org*, 2026. <https://ieeexplore.ieee.org/iel8/6287639/6514899/10930500.pdf> (accessed Apr. 29, 2026).
- [13] R. Yang, “A Novel Graph-Based Framework for Cryptocurrency Fraud Detection,” *Advances in Economics, Business and Management Research*, pp. 964–972, 2025, doi: https://doi.org/10.2991/978-94-6463-811-0_104.
- [14] Z. Zhao, J. Wang, and J. Wei, “Graph-Neural-Network-Based Transaction Link Prediction Method for Public Blockchain in Heterogeneous Information Networks,” *Blockchain: Research and Applications*, p. 100265, Jan. 2025, doi: <https://doi.org/10.1016/j.bcra.2024.100265>.
- [15] Y. Wang, Q. Zheng, X. Li, L. Wang, and L. Lin, “CoSemiGNN: Blockchain fraud detection with dynamic graph neural networks based on co-association of semi-supervised,” *Expert Systems with Applications*, vol. 298, p. 129853, Sep. 2025, doi: <https://doi.org/10.1016/j.eswa.2025.129853>.