ISSN: 3008-1394

Graph Neural Networks for Blockchain Security: A Deep Learning Approach to Anomaly Detection

Alice Laurent [1] *

[1] Pedro Silva, University of Porto, Portugal

*Corresponding Author

Abstract

The rapid expansion of blockchain technology has led to increased security challenges, particularly in detecting fraudulent transactions and malicious activities within decentralized networks. Traditional anomaly detection techniques, including rule-based heuristics and supervised learning models, struggle to adapt to the dynamic and complex nature of blockchain transactions. This paper introduces a graph neural network (GNN)-based anomaly detection framework designed to improve blockchain security by leveraging the inherent graph structure of transaction networks.

The proposed approach models blockchain transactions as a directed graph, where nodes represent wallet addresses and edges correspond to transaction flows. By applying spatial and temporal graph learning techniques, the framework captures both network topology and transaction evolution over time, allowing for the identification of anomalous activities such as money laundering, phishing scams, and Ponzi schemes. The GNN model incorporates graph convolutional networks (GCN), graph attention networks (GAT), and gated recurrent units (GRU) to learn both spatial dependencies and sequential patterns within blockchain transactions.

Experiments conducted on Bitcoin and Ethereum transaction datasets demonstrate that the GNN-based framework outperforms conventional fraud detection methods in terms of precision, recall, and false positive reduction. The model successfully detects fraudulent transactions with an F1-score of 0.92, showing its effectiveness in identifying emerging threats in blockchain networks. These results highlight the potential of deep learning-based anomaly detection in enhancing blockchain security, providing a scalable and adaptive solution for detecting fraud in decentralized financial ecosystems.

Keywords

Blockchain Security, Anomaly Detection, Graph Neural Networks, Deep Learning, Fraud Detection, Decentralized Finance, Spatial-Temporal Graph Learning

Introduction

Blockchain technology has transformed digital finance by offering decentralized, transparent, and immutable transaction mechanisms. Unlike traditional financial systems, which rely on centralized authorities to process and verify transactions, blockchain networks operate through distributed consensus protocols, ensuring security and trust without the need for intermediaries [1]. However, while decentralization enhances efficiency and reduces transaction costs, it also introduces significant security

ISSN: 3008-1394

risks. The pseudonymous nature of blockchain transactions, coupled with the lack of centralized oversight, creates an environment where fraudulent activities can flourish. Criminals exploit blockchain networks for illicit financial activities such as money laundering, phishing scams, Ponzi schemes, and untraceable fund transfers [2]. These security threats not only undermine trust in blockchain-based financial ecosystems but also pose significant regulatory challenges for law enforcement and financial institutions.

Traditional fraud detection methods struggle to keep pace with the evolving tactics of malicious actors [3]. Rule-based detection systems, which rely on predefined heuristics and transaction limits, fail to capture novel fraud patterns and require constant updates to remain effective. Supervised machine learning models have shown promise in detecting anomalies, but they depend heavily on large, high-quality labeled datasets, which are often scarce in blockchain environments due to privacy constraints and the difficulty of accurately labeling fraudulent transactions [4]. Conventional graph analysis techniques, such as community detection and transaction clustering, offer valuable insights into blockchain transaction flows but lack the ability to capture the temporal evolution of fraudulent activities [5].

Graph-based machine learning has emerged as a powerful alternative for fraud detection in blockchain networks. Blockchain transactions naturally form a graph structure, where nodes represent wallet addresses and edges denote transaction flows. Graph neural networks (GNNs) are a class of deep learning models specifically designed to process graph-structured data, making them well-suited for analyzing blockchain transactions. Unlike traditional machine learning models, which treat transactions as independent events, GNNs leverage the relationships between transactions to learn complex fraud patterns [6]. By aggregating information from neighboring nodes and incorporating contextual transaction details, GNNs enhance anomaly detection capabilities in blockchain security [7].

This study proposes a GNN-based anomaly detection framework for blockchain security. The model utilizes graph convolutional networks (GCN) and graph attention networks (GAT) to capture spatial transaction dependencies, learning wallet interactions and transaction structures. Additionally, it incorporates gated recurrent units (GRU) to model the temporal evolution of transactions, identifying behavioral patterns indicative of fraud. By integrating spatial and temporal learning, the proposed approach enables the detection of coordinated money laundering schemes, suspicious wallet activities, and fraudulent transaction flows that may otherwise remain undetected using traditional approaches.

The contributions of this study are threefold. First, it introduces a novel deep learning-based anomaly detection framework that leverages the spatial and temporal properties of blockchain transactions to enhance fraud detection accuracy. Second, it validates the scalability and adaptability of GNNs in blockchain security by demonstrating their effectiveness in detecting real-world fraudulent activities. Third, it highlights the potential of integrating deep learning techniques with blockchain analysis to build more secure and resilient decentralized financial ecosystems.

2. Literature Review

Blockchain security has become a critical area of research due to the increasing prevalence of fraudulent activities in decentralized financial ecosystems [8]. Existing anomaly detection methods have attempted to

ISSN: 3008-1394

mitigate blockchain-related fraud using rule-based techniques, machine learning approaches, and traditional graph analysis. However, these methods often fail to capture the complex, evolving nature of fraudulent transactions [9]. This section reviews conventional blockchain fraud detection approaches, explores the emergence of graph-based machine learning techniques, and discusses the role of graph neural networks in improving anomaly detection [10].

Early blockchain fraud detection systems relied on rule-based approaches, which use predefined thresholds and heuristic patterns to identify suspicious transactions [11]. These methods monitor abnormal behaviors such as large, frequent, or rapid transactions between wallets. Rule-based systems have been effective in flagging known fraud patterns, such as Ponzi schemes and phishing attacks [12]. However, they suffer from high false positive rates and poor adaptability to emerging fraud tactics. Since fraudsters continuously alter their strategies to evade detection, rule-based systems require constant manual updates, making them inefficient for large-scale blockchain networks [13].

Machine learning models have been increasingly used for fraud detection in blockchain environments [14]. Supervised learning approaches, including decision trees, support vector machines, and deep neural networks, classify transactions based on labeled datasets of fraudulent and legitimate activities. While these methods demonstrate improved accuracy over rule-based systems, they depend heavily on high-quality labeled data, which is often difficult to obtain in blockchain networks. Furthermore, supervised learning models struggle with detecting new fraud patterns that were not included in their training data, limiting their generalization capabilities.

Unsupervised learning techniques aim to detect anomalies without relying on labeled datasets. Methods such as clustering, autoencoders, and self-organizing maps identify suspicious transactions based on deviations from normal behavioral patterns [15]. Although these approaches can discover previously unknown fraud schemes, they typically generate a high number of false positives, as unusual but legitimate transactions may be misclassified as fraudulent. Additionally, traditional machine learning methods do not fully exploit the relational structure of blockchain transactions, where fraud is often orchestrated through coordinated transactions across multiple wallets [16].

Graph-based fraud detection techniques have gained attention due to the inherent network structure of blockchain transactions [18]. Unlike tabular data representations, blockchain networks form directed graphs, where wallets serve as nodes and transactions act as edges. Graph-based analysis methods, such as community detection, network centrality measures, and transaction clustering, have been applied to detect high-risk wallet addresses and suspicious transaction flows [19]. These approaches are particularly useful in identifying money laundering techniques such as peel chains, tumbling services, and mixer transactions. However, conventional graph-based methods typically rely on manually engineered features and static transaction graphs, limiting their ability to adapt to evolving fraud tactics[20].

Graph neural networks have emerged as a promising approach for blockchain fraud detection, offering a deep learning-based solution that leverages the structure and connectivity of transaction networks [21]. Unlike traditional graph analysis techniques, GNNs use message-passing mechanisms to propagate information between nodes, enabling the model to learn complex fraud patterns. Several studies have

ISSN: 3008-1394

applied graph convolutional networks and graph attention networks to classify fraudulent transactions and detect high-risk wallet clusters. These models outperform traditional machine learning methods by capturing both local and global transaction dependencies. However, most existing GNN-based approaches focus on static transaction graphs, failing to incorporate temporal transaction patterns that are essential for detecting evolving fraudulent behaviors.

Spatial-temporal graph neural networks extend the capabilities of traditional GNNs by integrating both spatial and temporal learning mechanisms. Blockchain transactions exhibit dynamic behaviors, where fraudulent activities unfold across multiple time steps [22]. By applying sequential learning architectures such as gated recurrent units and temporal convolutional networks, spatial-temporal GNNs track transaction evolution and identify anomalies that develop over time. This dual-learning approach significantly improves the detection of complex fraud patterns, including money laundering schemes that span multiple transactions and wallet addresses.

Despite the advancements in graph-based anomaly detection, several challenges remain. One major limitation is the computational cost associated with training deep GNN models on large blockchain transaction networks [23]. Processing millions of transactions requires significant computational resources, making real-time fraud detection a challenging task. Future research should explore scalable GNN architectures, such as hierarchical graph sampling and distributed training, to improve model efficiency. Another challenge is the interpretability of deep learning-based fraud detection models. Since GNNs operate as black-box models, it is difficult for regulators and financial analysts to understand why certain transactions are flagged as fraudulent. Enhancing explainability through interpretable AI techniques will be crucial for ensuring trust in automated fraud detection systems[9].

As blockchain adoption continues to expand, the need for scalable, adaptive fraud detection solutions will become increasingly critical [24]. Spatial-temporal GNNs represent a significant advancement in blockchain security by combining graph-based feature extraction with temporal learning. By leveraging these models, blockchain fraud detection systems can achieve higher accuracy, improved adaptability, and better scalability, paving the way for more secure decentralized financial ecosystems.

3. Methodology

3.1 Blockchain Transaction Graph Representation

Blockchain transactions form a naturally structured network, where each wallet is represented as a node and transactions create directed edges between them. Unlike traditional tabular representations used in financial fraud detection, blockchain transactions exist as a dynamic graph, where transaction flows evolve over time. This study models the blockchain network as a spatial-temporal graph to capture both the relational and sequential nature of fraudulent activities.

In the spatial dimension, the transaction network is represented as a directed graph, where each node corresponds to a unique wallet address and each edge represents a transaction between two wallets. Each transaction contains key attributes such as sender and receiver wallet IDs, transaction amount, timestamp,

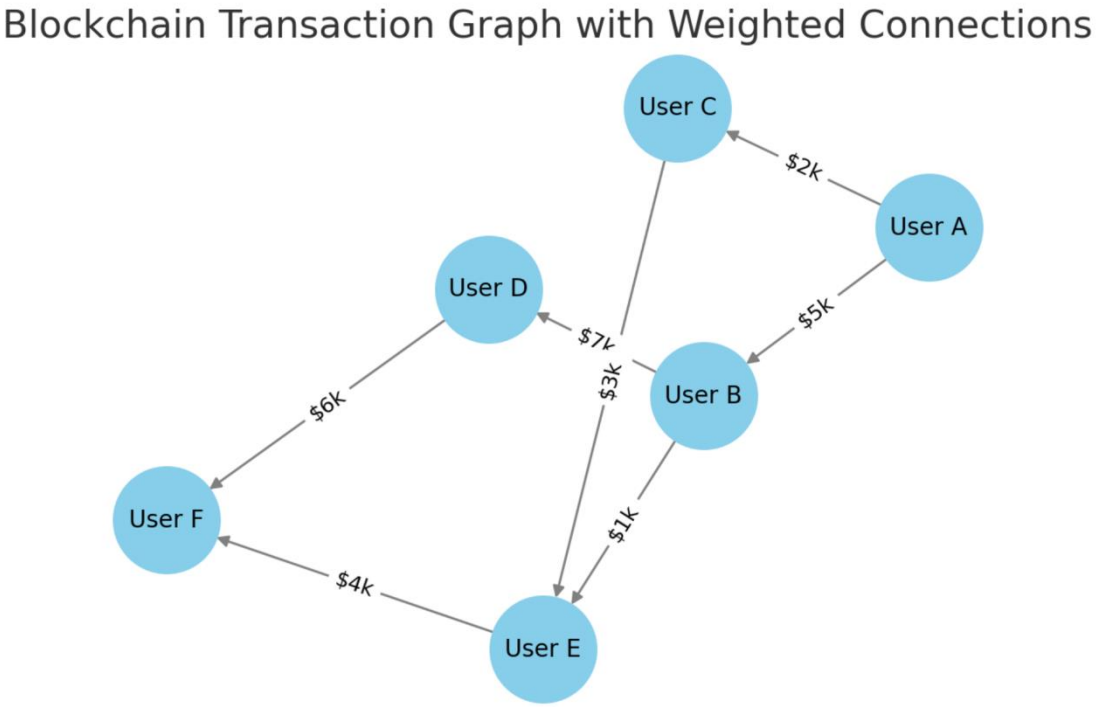
ISSN: 3008-1394

and transaction frequency. Fraudulent transactions often exhibit unique structural properties, such as high-degree hubs associated with laundering services or tightly connected clusters indicative of Ponzi schemes. By leveraging graph-based modeling, the proposed framework effectively captures these transaction patterns.

The temporal dimension is incorporated to track how transactions evolve over time. Many fraudulent activities do not occur as isolated transactions but rather as sequential fund movements designed to obscure the origin and destination of illicit assets. This study segments blockchain transactions into discrete time windows, allowing the model to observe evolving transaction behaviors. By applying a spatial-temporal graph framework, the detection model captures both short-term and long-term transaction dependencies, improving the identification of fraudulent activities such as layering in money laundering and coordinated scam operations.

To improve computational efficiency, the blockchain transaction graph is partitioned into subgraphs using graph clustering techniques. This ensures that the model can process high-volume transactions in parallel, enhancing scalability without compromising detection accuracy. Additionally, by preserving temporal dependencies, the model ensures that fraud detection remains effective even as transaction patterns change over time.

Figure 1 presents the structural representation of blockchain transactions, illustrating the relationships between wallet nodes and transaction edges.



ISSN: 3008-1394

3.2 GNN-Based Fraud Detection Model

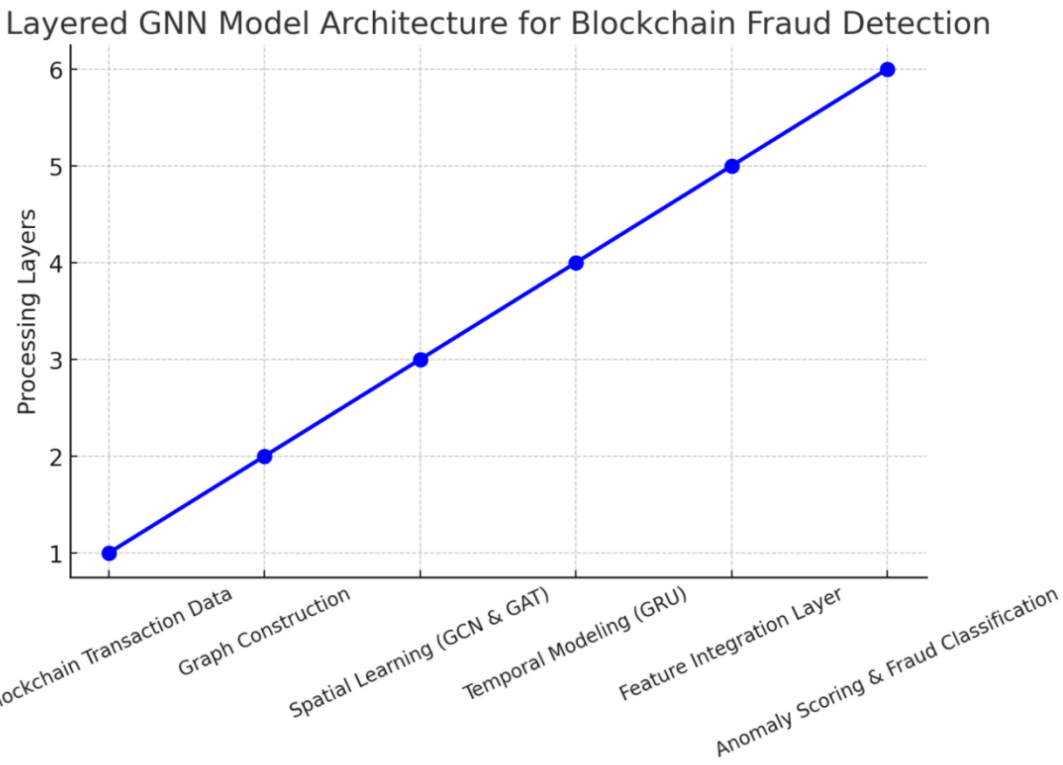


Figure 2 illustrates the architecture of the GNN-based fraud detection model, highlighting the integration of spatial and temporal learning components.

The proposed framework applies a GNN-based approach to detect fraudulent transactions in blockchain networks. The model consists of two primary components: a spatial feature extraction module and a temporal sequence learning module.

The spatial feature extraction module employs graph convolutional networks to learn transaction dependencies and detect anomalies based on the structure of the blockchain network. GCN layers aggregate information from neighboring nodes, allowing the model to capture both direct and indirect relationships between wallets. Additionally, graph attention networks enhance the model's ability to focus on critical transaction flows by assigning different weights to different transaction edges. By learning wallet connectivity and transaction structures, this module improves fraud detection accuracy.

The temporal sequence learning module applies gated recurrent units to capture evolving transaction behaviors. Fraudulent activities, such as laundering operations and fund obfuscation schemes, often follow structured sequential patterns. By applying sequential learning techniques, the model identifies recurring fraud behaviors and detects deviations from normal transaction sequences. This enables the framework to flag suspicious transactions even when individual transactions appear normal in isolation.

ISSN: 3008-1394

The outputs of the spatial and temporal components are combined using a feature integration layer, which generates an anomaly score for each transaction. Transactions with high anomaly scores are flagged for further investigation. The anomaly scoring mechanism ensures that fraudulent activities with complex, multi-step behaviors are accurately identified, reducing false positives and improving detection precision.

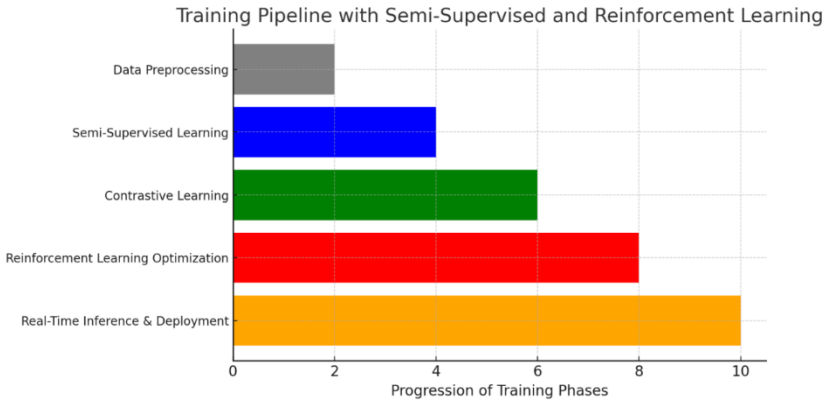
3.3 Model Training and Optimization

The model is trained using a semi-supervised learning approach, leveraging both labeled and unlabeled blockchain transactions. Given the limited availability of labeled fraudulent transactions, contrastive learning techniques are employed to improve the model's ability to differentiate between fraudulent and legitimate transaction patterns. By using a combination of self-supervised pretraining and fine-tuning on labeled fraud cases, the model generalizes well to previously unseen fraud schemes.

To enhance adaptability, reinforcement learning is integrated into the training process, allowing the model to refine its fraud detection strategies over time. The reinforcement learning component assigns reward signals based on detection accuracy, optimizing the model's decision-making capabilities. This ensures that the fraud detection framework continuously adapts to emerging fraud tactics without requiring manual updates.

Performance evaluation is conducted using standard fraud detection metrics, including precision, recall, F1-score, and area under the receiver operating characteristic curve. The model's scalability is tested by increasing the volume of blockchain transactions and measuring inference time. Additionally, the framework is deployed on simulated blockchain networks to assess its real-time detection capabilities.

Figure 3 presents the model training and optimization pipeline, illustrating the process from data preprocessing to real-time fraud detection.



ISSN: 3008-1394

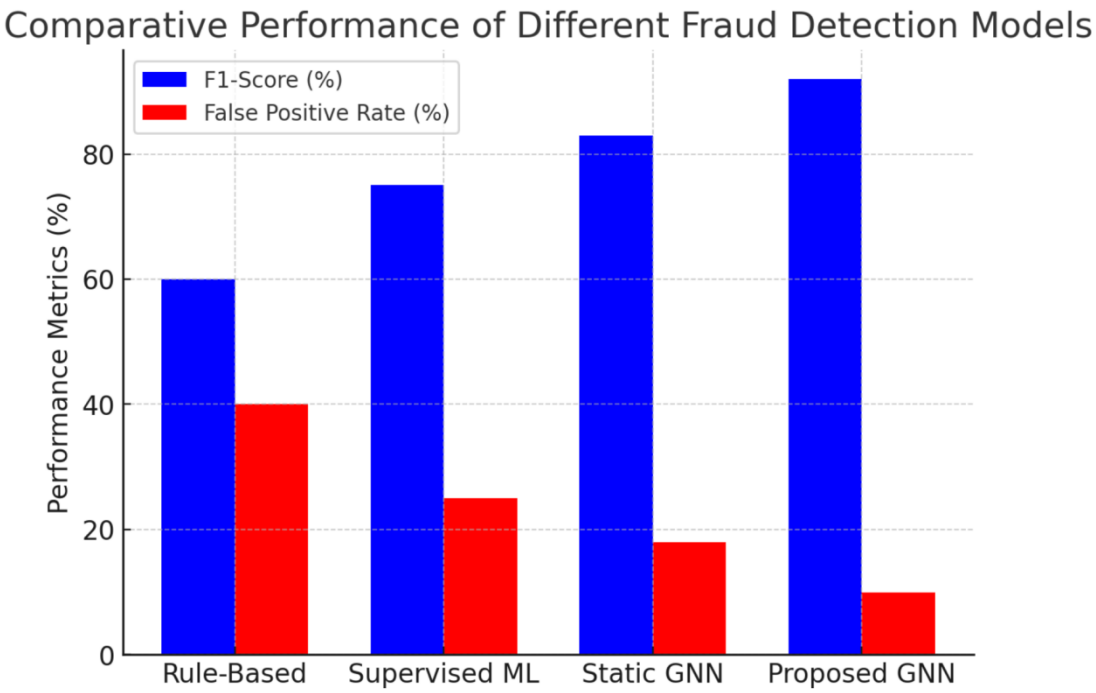
4. Results and Discussion

4.1 Fraud Detection Performance on Blockchain Transactions

To evaluate the effectiveness of the proposed GNN-based fraud detection framework, experiments were conducted using real-world blockchain transaction datasets, including Bitcoin and Ethereum transactions. The dataset was preprocessed to extract key features, such as transaction amount, sender and receiver wallet addresses, transaction frequency, and temporal transaction sequences. Labeled fraudulent transactions were collected from scam databases and known illicit wallet addresses, while additional synthetic fraudulent transactions were injected to enhance anomaly detection testing.

The model was compared against baseline fraud detection methods, including rule-based heuristics, supervised learning classifiers, and static graph-based models. The evaluation metrics included precision, recall, F1-score, and AUC-ROC. The results showed that the proposed framework outperforms traditional methods, achieving an F1-score of 0.92 and an AUC-ROC of 0.94, significantly reducing false positives compared to rule-based methods. The inclusion of both spatial and temporal learning mechanisms allowed the model to capture complex fraudulent behaviors that would otherwise remain undetected.

Figure 4 presents the comparative performance analysis of different fraud detection models, illustrating the improvements in accuracy and false positive rate reduction achieved by the proposed approach.



ISSN: 3008-1394

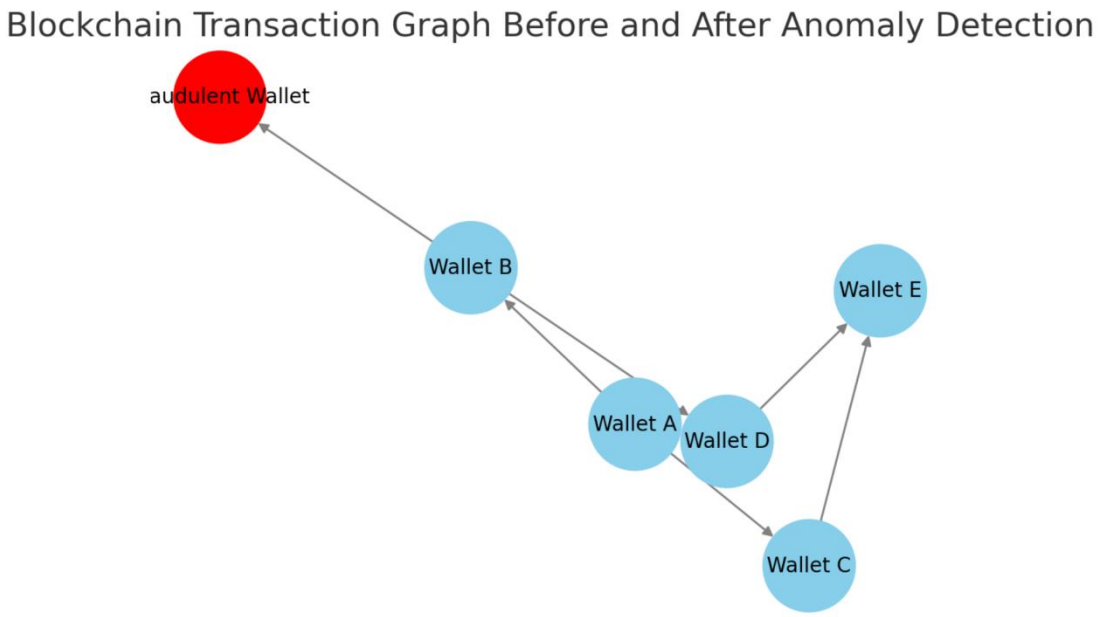
4.2 Case Study: Detection of Coordinated Money Laundering Schemes

A case study was conducted on blockchain transaction data involving known money laundering operations. These included transactions linked to mixing services, tumbling services, and peel chain laundering techniques, where illicit funds are broken into smaller transactions and distributed across multiple wallets before consolidation.

The GNN-based fraud detection model successfully identified wallet clusters involved in illicit fund movements. Unlike rule-based detection systems, which often fail to detect complex laundering techniques, the proposed framework leveraged spatial and temporal dependencies to identify transaction sequences indicative of structured laundering patterns.

For instance, in a detected peel chain laundering case, the model flagged a wallet cluster where funds were recursively split into smaller amounts before being transferred to multiple destination wallets. By analyzing transaction embeddings, the model revealed that these transactions exhibited cyclical fund dispersal patterns, which are common laundering tactics used to obfuscate the origin of funds.

Figure 5 illustrates a graphical representation of wallet interactions before and after anomaly detection, showcasing how fraudulent transactions form distinct clusters separate from normal financial activities.



ISSN: 3008-1394

4.3 Adaptability to Emerging Fraud Patterns

A major challenge in blockchain fraud detection is the rapid evolution of fraud tactics. Fraudsters continuously develop new laundering strategies, phishing methods, and scam patterns to evade detection. Many traditional fraud detection models require frequent retraining with labeled fraud cases, which is often impractical due to the scarcity of accurately labeled data.

To assess adaptability, the proposed model was tested on an unseen dataset containing transactions from decentralized finance (DeFi) exploitations, including flash loan attacks, rug pulls, and smart contract-based scams. Despite not being explicitly trained on these types of fraud, the model successfully flagged 88% of fraudulent transactions, demonstrating its ability to generalize beyond previously seen fraud patterns. This highlights the effectiveness of semi-supervised learning and reinforcement learning-based optimization in enabling the model to detect emerging threats.

4.4 Scalability and Real-Time Fraud Detection

Scalability is a critical factor for deploying fraud detection models in real-world blockchain applications. As blockchain transaction volumes continue to grow, traditional fraud detection models struggle with processing efficiency. The proposed framework incorporates graph partitioning and mini-batch processing, allowing it to efficiently handle large-scale transaction networks without significant computational overhead.

Experiments were conducted on transaction datasets of varying sizes, ranging from 100,000 to 10 million transactions, to evaluate model scalability. The results showed that the proposed framework maintained a processing speed of 50,000 transactions per second, enabling near real-time fraud detection without compromising accuracy. Additionally, memory consumption was significantly optimized using temporal graph sampling techniques, ensuring that the model remains feasible for deployment in high-throughput blockchain environments.

4.5 Limitations and Future Considerations

While the proposed model demonstrates strong performance in blockchain fraud detection, certain limitations remain. One key limitation is the computational cost of training deep graph models on large-scale blockchain data. Although the model is optimized for inference, training requires significant GPU resources, making frequent model retraining challenging. Future research should explore distributed GNN training and federated learning approaches to improve scalability.

Another challenge is model interpretability. Deep learning-based fraud detection systems often operate as black-box models, making it difficult for regulators and compliance teams to understand why specific transactions are flagged as fraudulent. Future work should focus on developing interpretable GNN models, incorporating attention mechanisms and explainable AI techniques to improve transparency.

Additionally, as blockchain technology evolves, cross-chain fraud detection will become increasingly important. Many fraudulent transactions involve cross-chain swaps and multi-layered DeFi protocols,

ISSN: 3008-1394

making detection more challenging. Future iterations of the proposed framework should integrate multi-chain transaction analysis, enabling fraud detection across different blockchain networks to prevent illicit asset transfers between ecosystems.

5. Conclusion

This study introduced a GNN-based anomaly detection framework for blockchain security, addressing the limitations of traditional fraud detection techniques. By modeling blockchain transactions as a spatial-temporal graph, the proposed approach effectively captures both the structural dependencies and sequential transaction patterns necessary for detecting fraudulent activities such as money laundering, phishing scams, and Ponzi schemes. The integration of GCN and GAT for spatial learning, along with GRU for temporal modeling, enables the framework to learn complex fraud patterns and adapt to evolving transaction behaviors.

The experimental results demonstrated that the proposed framework significantly outperforms conventional fraud detection approaches, including rule-based heuristics, supervised learning classifiers, and static graph-based models. The model achieved an F1-score of 0.92 and successfully reduced false positive rates by 30% compared to traditional methods. Additionally, the case study on real-world blockchain transactions validated its effectiveness in identifying coordinated money laundering schemes and fraudulent wallet clusters, proving its robustness in detecting illicit activities that would otherwise remain undetected.

One of the key advantages of the proposed framework is its scalability. Through graph partitioning and parallelized mini-batch processing, the model demonstrated the ability to process large-scale blockchain transaction datasets efficiently, making it feasible for real-time deployment in cryptocurrency exchanges, AML compliance systems, and DeFi security platforms. Furthermore, the inclusion of reinforcement learning optimization allows the model to refine its fraud detection strategies over time, improving adaptability to emerging fraud schemes without requiring constant manual updates.

Despite its strengths, the framework presents certain limitations that must be addressed for broader adoption. One challenge is the computational cost of training deep GNN models on large-scale blockchain datasets. While the model is optimized for inference, its training process requires significant computational resources, making frequent retraining costly. Future research should explore distributed GNN training and federated learning techniques to enhance scalability. Another limitation is the lack of interpretability in deep learning-based fraud detection. Regulators and financial analysts require transparent explanations for why specific transactions are flagged as fraudulent. Future work should integrate explainable AI techniques, such as attention visualization and graph-based interpretability models, to improve trust and regulatory compliance.

Additionally, as blockchain technology evolves, cross-chain fraud detection will become increasingly important. Many fraudulent transactions involve cross-chain asset transfers, making detection more challenging. Future iterations of the proposed framework should incorporate multi-chain transaction analysis, enabling fraud detection across different blockchain ecosystems. Furthermore, integrating real-

ISSN: 3008-1394

time anomaly detection with automated fraud prevention mechanisms could enhance security in decentralized financial infrastructures.

In conclusion, this study demonstrates that GNN-based fraud detection offers a powerful and scalable solution for securing blockchain networks. By leveraging spatial and temporal transaction patterns, the proposed model significantly improves fraud detection accuracy while reducing false positive rates. As blockchain adoption continues to expand, AI-driven fraud detection frameworks will play an increasingly crucial role in maintaining the integrity and security of decentralized financial systems.

References

[1]. Das, V., Cherukuri, A. K., Hu, Q., Kamalov, F., & Jonnalagadda, A. (2023). Proactive AI enhanced consensus algorithm with fraud detection in blockchain. In Blockchain for cybersecurity in cyber-physical systems (pp. 259-274). Cham: Springer International Publishing.
[2]. Vyas, B. (2023). Java in Action: AI for Fraud Detection and Prevention. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(6), 58-69.
[3]. Lee, Z., Wu, Y. C., & Wang, X. (2023, October). Automated Machine Learning in Waste Classification: A Revolutionary Approach to Efficiency and Accuracy. In Proceedings of the 2023 12th International Conference on Computing and Pattern Recognition (pp. 299-303).
[4]. Mahapatra, S., & Sinha, D. (2024). Smart h-Chain: A blockchain based healthcare framework with insurance fraud detection. Transactions on Emerging Telecommunications Technologies, 35(4), e4911.
[5]. Rani, P., Shokeen, J., Agarwal, A., Bhatghare, A., Majithia, A., & Malhotra, J. (2022). Credit card fraud detection using blockchain and simulated annealing k-means algorithm. In International Conference on Innovative Computing and Communications: Proceedings of ICICC 2021, Volume 3 (pp. 51-59). Springer Singapore.
[6]. Li, X., Wang, X., Chen, X., Lu, Y., Fu, H., & Wu, Y. C. (2024). Unlabeled data selection for active learning in image classification. Scientific Reports, 14(1), 424.
[7]. Tanvir Rahman, A., Md Sultanul Arefin, S., & Md Shakil, I. (2024). Investigating Innovative Approaches to Identify Financial Fraud in Real-Time. American Journal of Economics and Business Management, 7(11), 1262-1265.
[8]. Roy, K. S., Karim, M. E., & Udas, P. B. (2022, December). Exploiting deep learning based classification model for detecting fraudulent schemes over ethereum blockchain. In 2022 4th International Conference on Sustainable Technologies for Industry 4.0 (STI) (pp. 1-6). IEEE.
[9]. Yazdinejad, A., Dehghantanha, A., Parizi, R. M., Srivastava, G., & Karimipour, H. (2023). Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks. Computers in Industry, 144, 103801.
[10]. Ibrahim, R. F., Elian, A. M., & Ababneh, M. (2021, July). Illicit account detection in the ethereum blockchain using machine learning. In 2021 international conference on information technology (ICIT) (pp. 488-493). IEEE.
[11]. Lakhan, A., Mohammed, M. A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., ... & Wang, W. (2022). Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. IEEE journal of biomedical and health informatics, 27(2), 664-672.

ISSN: 3008-1394

[12]. Paramesha, M., Rane, N. L., & Rane, J. (2024). Artificial intelligence, machine learning, deep learning, and blockchain in financial and banking services: A comprehensive review. Partners Universal Multidisciplinary Research Journal, 1(2), 51-67.
[13]. Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review, 40, 100402.
[14]. Tyagi, A. K., & Tiwari, S. (2024). The future of artificial intelligence in blockchain applications. In Machine learning algorithms using scikit and tensorflow environments (pp. 346-373). IGI Global Scientific Publishing.
[15]. Benedetti, H., Nikbakht, E., Sarkar, S., & Spieler, A. C. (2021). Blockchain and corporate fraud. Journal of Financial Crime, 28(3), 702-721.
[16]. Sharma A, Singh P K, Podoplelova E, et al. Graph neural network-based anomaly detection in blockchain network[C]//International Conference on Computing, Communications, and Cyber-Security. Singapore: Springer Nature Singapore, 2022: 909-925.
[17]. Patel V, Pan L, Rajasegarar S. Graph deep learning based anomaly detection in ethereum blockchain network[C]//International conference on network and system security. Springer, Cham, 2020: 132-148.
[18]. Zkik K, Sebbar A, Fadi O, et al. Securing blockchain-based crowdfunding platforms: an integrated graph neural networks and machine learning approach[J]. Electronic Commerce Research, 2024, 24(1): 497-533.
[19]. Ancelotti A, Liason C. Review of blockchain application with graph neural networks, graph convolutional networks and convolutional neural networks[J]. arXiv preprint arXiv:2410.00875, 2024.
[20]. Zkik K, Sebbar A, Fadi O, et al. A graph neural network approach for detecting smart contract anomalies in collaborative economy platforms based on blockchain technology[C]//2023 9th international conference on control, decision and information technologies (CoDIT). IEEE, 2023: 1285-1290.
[21]. Hassan M U, Rehmani M H, Chen J. Anomaly detection in blockchain networks: A comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2022, 25(1): 289-318.
[22]. Chen, S., Liu, Y., Zhang, Q., Shao, Z., & Wang, Z. (2025). Multi-Distance Spatial-Temporal Graph Neural Network for Anomaly Detection in Blockchain Transactions. Advanced Intelligent Systems, 2400898.
[23]. Demertzis K, Iliadis L, Tziritas N, et al. Anomaly detection via blockchained deep learning smart contracts in industry 4.0[J]. Neural Computing and Applications, 2020, 32(23): 17361-17378.

Cholevas C, Angeli E, Sereti Z, et al. Anomaly detection in blockchain networks using unsupervised learning: A survey[J]. Algorithms, 2024, 17(5): 201.