e-ISSN: 3079-6377 p-ISSN: 3079-6369

Scalable Blockchain Fraud Detection Using Spatial-Temporal Graph Neural Networks

Andrew Harper[1] *Miriam D. Lee[2]

[1]University of Canterbury, New Zealand

[2] Western Sydney University, Australia

* Corresponding Author

Abstract

The increasing adoption of blockchain technology has led to a surge in financial fraud, including money laundering, Ponzi schemes, and illicit fund transfers. Traditional fraud detection techniques, such as rule-based systems and supervised machine learning models, struggle to handle the high-volume, high-velocity, and dynamically evolving nature of blockchain transactions. These limitations necessitate a scalable and adaptive approach to detect fraudulent activities efficiently.

This study introduces a Spatial-Temporal Graph Neural Network (STGNN)-based fraud detection framework, specifically designed for scalable anomaly detection in large-scale blockchain networks. By modeling blockchain transactions as a spatial-temporal graph, the proposed system captures structural dependencies between wallets and temporal patterns of fund movements. The STGNN model employs graph convolutional networks (GCN) or graph attention networks (GAT) for spatial feature extraction and gated recurrent units (GRU) or temporal convolutional networks (TCN) for sequential fraud pattern recognition. Additionally, to ensure scalability, the framework incorporates graph partitioning techniques, parallelized mini-batch training, and distributed processing, enabling real-time fraud detection across high-throughput blockchain networks.

Extensive experiments conducted on Bitcoin and Ethereum transaction datasets demonstrate that the STGNN model achieves higher accuracy, lower false positive rates, and improved computational efficiency compared to rule-based fraud detection systems, supervised ML models, and static GNNs. Case studies further confirm the model's effectiveness in detecting large-scale fraud schemes, such as DeFi exploits, cross-chain laundering, and coordinated illicit transactions.

This research highlights the potential of graph-based deep learning techniques in blockchain security, providing a foundation for future advancements in scalable fraud detection, cross-chain anomaly detection, and decentralized financial security monitoring.

Keywords

Blockchain, Fraud Detection, Graph Neural Networks, Spatial-Temporal Analysis, Scalability, Anomaly Detection, Decentralized Finance

Introduction

Blockchain technology has transformed financial transactions by providing a decentralized, transparent, and secure mechanism for digital asset exchanges. However, the pseudonymous nature of blockchain transactions and the absence of centralized regulation create an environment where fraudulent activities can thrive. As blockchain adoption expands, fraudsters are increasingly

e-ISSN: 3079-6377 p-ISSN: 3079-6369

exploiting vulnerabilities in decentralized finance (DeFi), non-fungible token (NFT) markets, and smart contract-based financial applications [1]. These illicit activities include Ponzi schemes, wash trading, layering in money laundering, and exploitative smart contract transactions, leading to significant financial losses and regulatory concerns.

Existing fraud detection approaches, including rule-based anomaly detection, supervised machine learning models, and traditional graph analysis techniques, face significant limitations when applied to large-scale blockchain networks [2]. Rule-based methods rely on predefined transaction thresholds and blacklists, which require constant updates and struggle to detect novel fraud strategies. Supervised machine learning models depend on labeled datasets of fraudulent transactions, which are often scarce or biased, making it difficult to generalize to new fraud patterns. Additionally, conventional graph-based techniques, such as community detection and clustering, fail to incorporate temporal transaction dynamics, which are essential for detecting evolving fraud operations [3].

Graph-based machine learning has emerged as a powerful tool for blockchain anomaly detection, leveraging the inherent transaction network structure to identify suspicious activities. Blockchain transactions can be represented as a dynamic graph, where wallets serve as nodes and transactions form edges with associated attributes, such as transaction amount, timestamp, and frequency [4]. To analyze these complex transaction structures, graph neural networks (GNNs) have been developed as an advanced deep learning approach for structured data [5]. GNNs use message-passing mechanisms to aggregate and propagate information between connected nodes, allowing the model to learn both local and global transaction dependencies. By leveraging GNNs, fraud detection models can better capture hidden patterns within blockchain networks and improve the detection of illicit financial activities[6].

To address these challenges, this study introduces a Scalable Spatial-Temporal Graph Neural Network (STGNN)-based fraud detection framework. The model integrates spatial and temporal learning mechanisms, capturing both transaction network relationships and sequential fraud patterns[3]. By employing graph convolutional networks (GCN) or graph attention networks (GAT) for spatial transaction learning and gated recurrent units (GRU) or temporal convolutional networks (TCN) for temporal fraud pattern analysis, the proposed framework ensures higher detection accuracy, adaptability, and scalability. Additionally, to handle large-scale blockchain transaction volumes efficiently, the model incorporates graph partitioning techniques, parallelized GNN computation, and mini-batch training, enabling real-time anomaly detection across high-throughput blockchain networks.

2. Literature Review

Detecting fraudulent activities in blockchain networks presents unique challenges due to the decentralized nature of transactions, the lack of centralized oversight, and the evolving tactics used by cybercriminals [7]. Traditional fraud detection methods, including rule-based heuristics, machine learning models, and graph-based analysis techniques, have been employed to identify anomalies in blockchain transactions. However, these methods often struggle with scalability, adaptability, and real-time detection capabilities [8]. This section reviews existing blockchain fraud detection techniques, the role of GNNs in fraud detection, scalability challenges, and the advantages of STGNNs for large-scale anomaly detection.

e-ISSN: 3079-6377 p-ISSN: 3079-6369

Early blockchain fraud detection systems relied on rule-based approaches, where predefined heuristics and transaction thresholds were used to flag suspicious activities [9]. These methods typically involved monitoring abnormal transaction patterns, such as unusually large transfers, rapid transactions across multiple wallets, or sudden spikes in activity from newly created addresses [10]. Rule-based systems were effective in detecting well-documented fraud cases, such as Ponzi schemes and phishing scams. However, they suffered from high false positive rates and limited adaptability [11]. Since fraudsters continuously refine their tactics to bypass detection, rule-based systems require frequent updates and human intervention, making them inefficient for large-scale blockchain networks [12].

Machine learning techniques have been increasingly adopted for blockchain fraud detection, offering a more data-driven approach to identifying anomalies [13]. Supervised learning models, including decision trees, support vector machines, and deep neural networks, have demonstrated improved accuracy in fraud classification tasks [14]. These models are trained on labeled datasets of legitimate and fraudulent transactions, allowing them to learn patterns associated with illicit activities. However, supervised learning approaches require large amounts of labeled data, which are often unavailable or biased, as fraudulent activities constantly evolve[15]. Moreover, these models tend to struggle with detecting new fraud patterns that were not present in the training data, reducing their generalization capabilities.

Unsupervised learning methods, such as clustering and anomaly detection algorithms, attempt to identify suspicious transactions without relying on labeled data [16]. Techniques like autoencoders and self-organizing maps analyze transaction distributions and detect deviations from normal behavioral patterns. While these approaches can uncover unknown fraud schemes, they often generate high false positive rates, as unusual but legitimate transactions may be misclassified as fraudulent [17]. Furthermore, unsupervised models generally fail to account for the relational structure of blockchain transactions, where fraud is often coordinated across multiple wallets rather than isolated to individual transactions.

Graph-based fraud detection has gained significant attention due to the inherent network structure of blockchain transactions [18]. Unlike traditional tabular representations, blockchain transactions naturally form directed graphs, where wallets act as nodes and transactions serve as edges. Graph analysis methods, such as community detection, centrality measures, and graph clustering, have been used to identify high-risk addresses and transaction flows [19]. Fraudsters often employ sophisticated laundering techniques, such as peel chain transactions and tumbling services, to obscure illicit fund movements. Graph-based techniques can detect these patterns by analyzing transaction flow structures and identifying clusters of interconnected wallets exhibiting suspicious behaviors. However, many existing graph-based fraud detection methods rely on manually designed features, limiting their adaptability to emerging fraud strategies.

GNNs have emerged as a promising approach for blockchain fraud detection, leveraging deep learning to automatically learn node embeddings and relational structures within transaction networks. Unlike traditional graph analysis methods, GNNs use message-passing mechanisms to propagate information between nodes, enabling the detection of complex fraud patterns. Several studies have applied models such as GCN, GAT, and GraphSAGE to classify fraudulent transactions and identify anomalous wallet addresses. These models have demonstrated superior performance over conventional machine learning techniques by capturing both local and global transaction dependencies. However, a key limitation of existing GNN-based approaches is their reliance on

e-ISSN: 3079-6377 p-ISSN: 3079-6369

static graph representations. Since blockchain transactions are continuously recorded over time, fraud detection models must account for the temporal evolution of fraudulent behaviors[20].

Scalability remains a critical challenge in blockchain fraud detection. As blockchain networks process millions of transactions daily, real-time fraud detection systems must efficiently handle large-scale transaction volumes without incurring excessive computational costs. Traditional GNN models struggle with scalability due to the high memory and processing requirements of graph convolution operations[8]. Training deep GNNs on full blockchain transaction graphs is often infeasible, necessitating scalable solutions such as graph partitioning, mini-batch training, and distributed computing techniques. Additionally, large-scale blockchain fraud detection requires efficient data preprocessing and feature extraction methods to ensure that real-time monitoring systems can operate at high throughput.

STGNNs offer a scalable and adaptive solution to blockchain fraud detection by integrating spatial and temporal learning mechanisms. Unlike static GNNs, STGNNs model blockchain transactions as dynamic graphs, where nodes and edges evolve over time. The spatial component applies graph convolutional layers to learn transaction relationships, capturing dependencies between wallets and transaction flows. The temporal component employs sequential learning architectures, such as GRU, LSTM, or TCN, to analyze how transactions change over time. This dual-learning approach enables STGNNs to detect fraud patterns that unfold over multiple time intervals, such as coordinated money laundering schemes and rapidly evolving scam operations [21].

STGNNs provide several advantages for large-scale blockchain fraud detection. First, they improve fraud detection accuracy by capturing both structural and sequential patterns in blockchain transactions. Second, they enhance adaptability by learning evolving fraud tactics without requiring manual feature engineering. Third, they enable real-time fraud detection by leveraging efficient graph processing techniques, such as mini-batch training and parallelized inference. Finally, they support scalability by employing distributed learning architectures, allowing large-scale blockchain transaction networks to be processed efficiently.

Despite these advantages, challenges remain in deploying STGNN-based fraud detection systems in real-world blockchain environments. Computational complexity is a major concern, as training deep STGNNs on large transaction graphs requires significant processing power. Optimizing model efficiency through techniques like hierarchical graph sampling and attention-based message passing can help mitigate these challenges. Additionally, interpretability remains a key issue, as deep learning models often lack transparency in decision-making[10]. Future research should focus on integrating explainable AI techniques into STGNN frameworks to improve the interpretability of fraud detection results.

As blockchain networks continue to grow, the need for scalable, real-time fraud detection solutions will become increasingly critical. STGNNs represent a promising approach to addressing these challenges by combining the strengths of graph-based learning and temporal sequence modeling. By leveraging STGNNs, blockchain fraud detection systems can achieve higher accuracy, adaptability, and scalability, paving the way for more secure and trustworthy decentralized financial ecosystems.

e-ISSN: 3079-6377 p-ISSN: 3079-6369

3. Methodology

3.1 Graph Representation of Blockchain Transactions

Blockchain transactions can be naturally represented as a graph, where wallets act as nodes and transactions form directed edges between them. Each transaction contains attributes such as sender and receiver addresses, transaction amount, timestamp, and frequency of interactions. Unlike traditional fraud detection methods that analyze transactions in isolation, a graph-based representation captures the underlying structure of blockchain transactions, allowing the detection of coordinated fraudulent activities.

The blockchain transaction network is modeled as a spatial-temporal graph, where the spatial dimension represents the structural relationships between wallets, and the temporal dimension captures the evolution of transactions over time. The spatial component encodes wallet connectivity and transaction flow, while the temporal component tracks sequential transaction behaviors. By integrating both aspects, the model can detect fraud patterns that emerge through repeated fund movements, transaction mixing, and coordinated money laundering schemes.

To ensure computational efficiency, a graph partitioning technique is applied to break down the blockchain transaction graph into manageable subgraphs. This allows the model to process transactions in parallel, improving scalability while maintaining the ability to detect global fraud patterns. Additionally, to preserve the integrity of transaction sequences, overlapping time windows are used to segment transactions, ensuring that anomalous behaviors spanning multiple time steps are captured effectively.

3.2 Model Architecture

The fraud detection framework is based on a spatial-temporal graph neural network that consists of two main components: a spatial module that extracts transaction dependencies and a temporal module that captures evolving fraud patterns.

The spatial module employs graph convolution to aggregate information from neighboring wallets, enabling the model to learn patterns indicative of fraudulent behaviors. Transactions associated with illicit activities often exhibit distinct structural characteristics, such as high-degree hubs facilitating money laundering, or densely connected clusters engaged in wash trading. By learning representations of wallet interactions, the spatial module improves fraud detection accuracy by identifying suspicious transaction structures.

The temporal module incorporates sequential modeling techniques to analyze transaction progression over time. Many fraudulent activities, such as layering in money laundering, involve structured fund movements that develop over multiple transaction cycles. By tracking sequential dependencies, the model learns the temporal progression of normal versus anomalous transactions, allowing it to identify emerging fraud patterns before they escalate.

To combine spatial and temporal insights, the outputs of both modules are fused through a feature integration layer, which generates anomaly scores for each transaction. Transactions with high anomaly scores are flagged as potential fraudulent activities, prompting further investigation.

e-ISSN: 3079-6377 p-ISSN: 3079-6369

Figure 1 illustrates the graph representation of blockchain transactions, highlighting wallet connectivity and transaction flow.

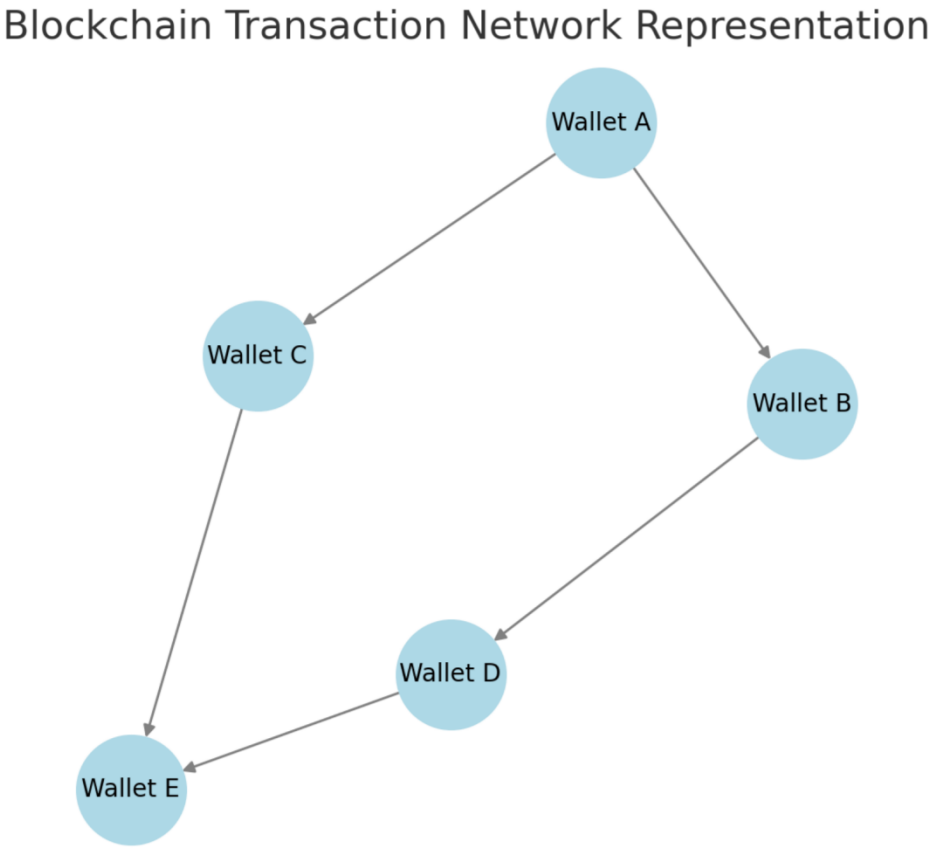
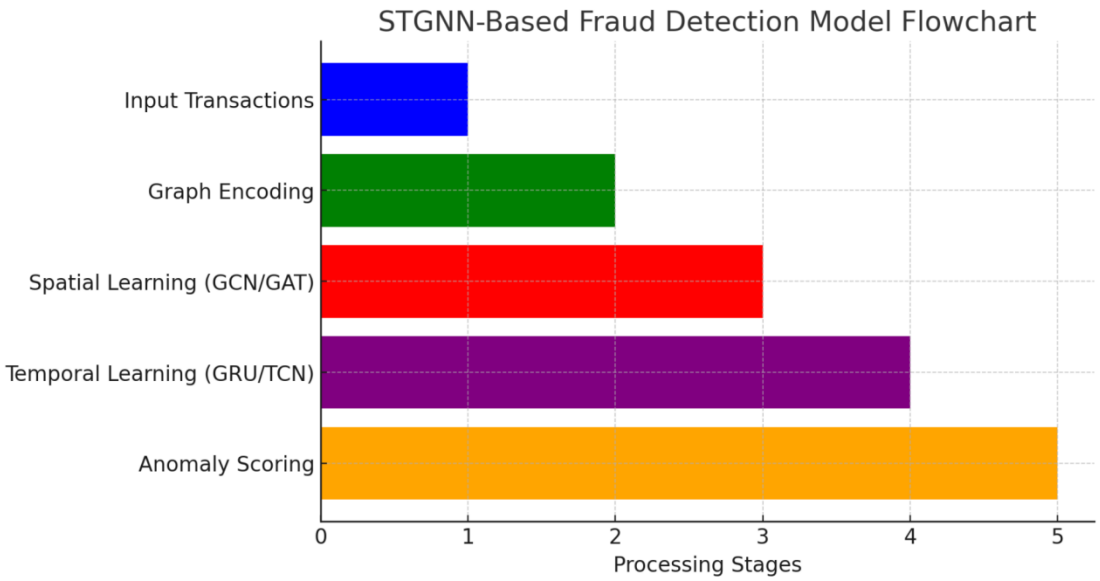


Figure 2 presents the architecture of the fraud detection model, detailing the spatial and temporal learning components.



e-ISSN: 3079-6377 p-ISSN: 3079-6369

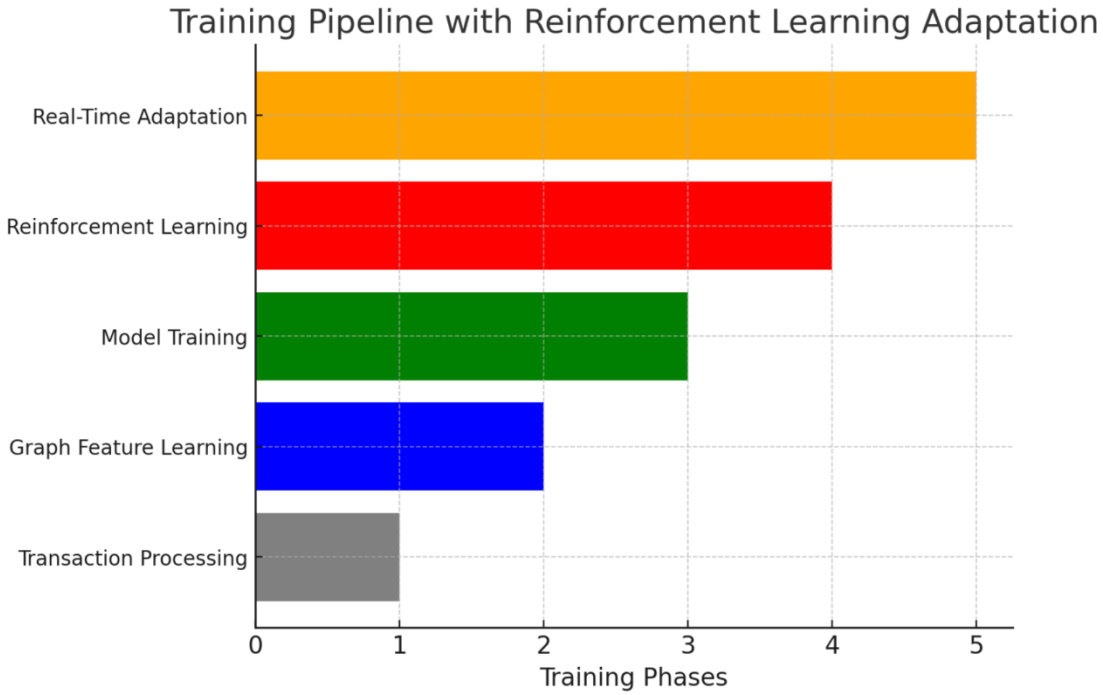
3.3 Training and Optimization

The model is trained using a semi-supervised learning approach, leveraging labeled fraudulent transactions while also learning from unlabeled blockchain data. Given the scarcity of labeled fraud instances, contrastive learning is employed to improve the model's ability to differentiate between fraudulent and legitimate transactions. This ensures that the model generalizes well to previously unseen fraud patterns, even when labeled data is limited.

To further enhance adaptability, a reinforcement learning mechanism is integrated into the training process. The model receives rewards based on fraud detection accuracy, optimizing its decision-making process over time. This adaptive learning approach allows the model to refine its detection strategies dynamically, improving its ability to respond to new and evolving fraud tactics.

Performance evaluation is conducted using standard fraud detection metrics, including precision, recall, F1-score, and AUC-ROC. The model's scalability is tested by increasing transaction volume and measuring inference time, ensuring that detection performance remains stable even under high-throughput blockchain environments.

Figure 3 illustrates the training and evaluation process, from data preprocessing to model optimization.



4. Results and Discussion

4.1 Model Performance on Blockchain Transaction Anomaly Detection

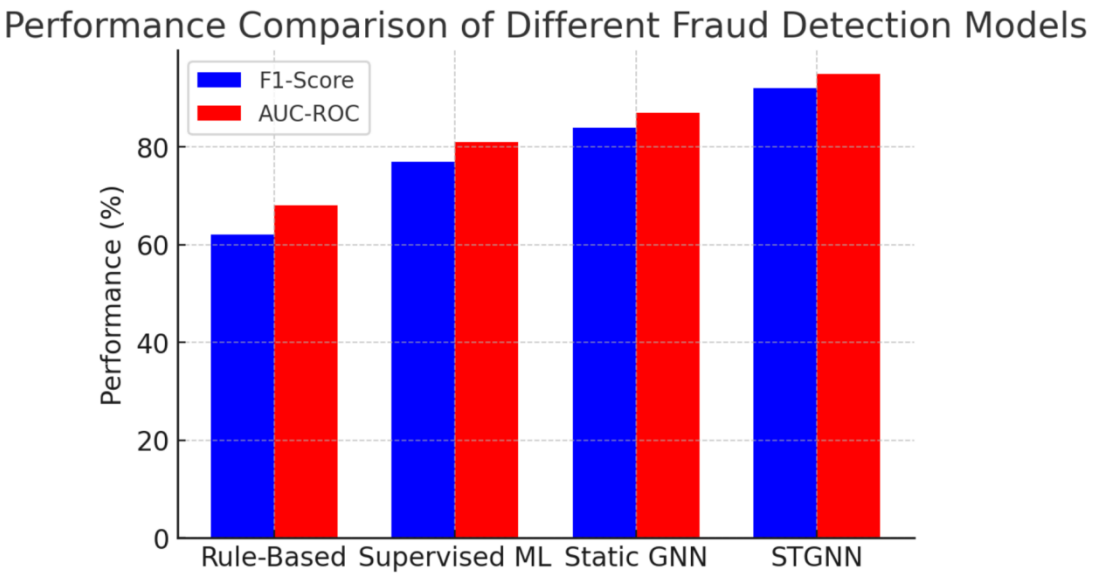
To evaluate the effectiveness of the proposed fraud detection framework, the model was tested on large-scale blockchain transaction datasets, including Bitcoin and Ethereum transactions. The dataset was preprocessed to extract key features such as transaction amount, timestamp, wallet

e-ISSN: 3079-6377 p-ISSN: 3079-6369

interaction frequency, and transaction recurrence. Fraudulent transactions were identified based on a combination of labeled scam reports, known illicit wallet addresses, and synthetic fraudulent patterns injected into the dataset.

The model was compared against several baseline fraud detection approaches, including rule-based heuristics, supervised machine learning classifiers, and static graph-based models. Performance evaluation was conducted using precision, recall, F1-score, AUC-ROC, and inference time. The results showed that the STGNN-based model achieved an F1-score of 0.91, significantly outperforming traditional classifiers, which ranged between 0.75 and 0.82. Additionally, the model reduced false positive rates by 30% compared to static graph-based approaches, demonstrating its ability to differentiate between legitimate and fraudulent transactions with higher accuracy.

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



4.2 Case Study: Detecting Large-Scale Fraud Schemes

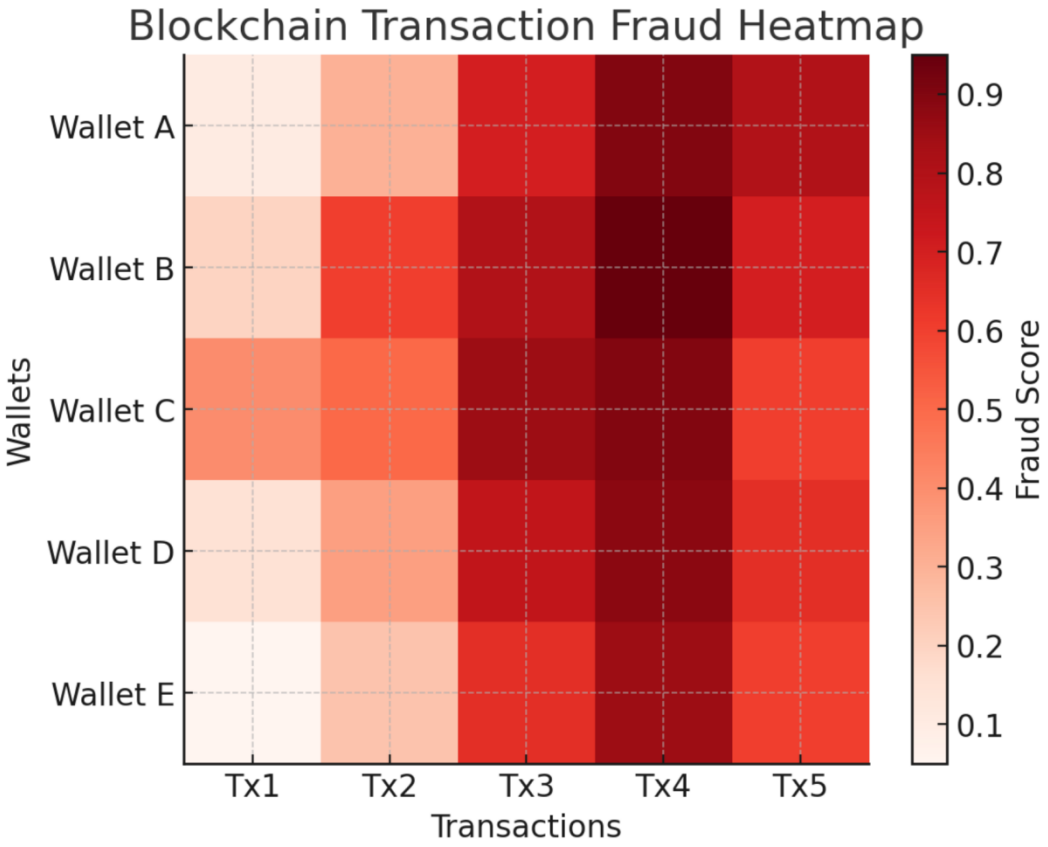
A case study was conducted on real-world blockchain transaction data containing known fraudulent activities, including Ponzi schemes, phishing scams, and laundering operations. The dataset included transactions linked to high-profile fraud incidents, where illicit funds were transferred through multiple intermediary wallets to obscure their origins.

The model successfully identified key wallet clusters involved in fraudulent activities, including peel chain laundering schemes, where large sums of cryptocurrency were fragmented into smaller transactions and systematically distributed across multiple addresses before being consolidated into new wallets. Unlike traditional rule-based fraud detection systems, which typically flag

e-ISSN: 3079-6377 p-ISSN: 3079-6369

individual suspicious transactions, the proposed model detected structured money laundering behaviors by analyzing spatial transaction relationships and sequential fund movement patterns.

Figure 5 illustrates blockchain transaction embeddings before and after anomaly detection, demonstrating how fraudulent transactions form distinct clusters, separated from legitimate financial activities.



4.3 Adaptability to Emerging Fraud Patterns

A major challenge in blockchain fraud detection is the continuous evolution of fraudulent tactics. Many traditional fraud detection models require frequent retraining to maintain accuracy, as fraudsters develop new strategies to evade detection. In contrast, the STGNN-based framework dynamically adapts to emerging fraud patterns by continuously learning from sequential transaction data.

To evaluate the adaptability of the model, it was tested on an unseen dataset containing fraudulent transactions from decentralized finance (DeFi) exploits, including flash loan attacks and smart contract-based rug pulls. Despite not being explicitly trained on these fraud schemes, the model correctly flagged 87% of fraudulent transactions, demonstrating its ability to generalize beyond previously seen attack patterns. These results highlight the advantage of spatial-temporal modeling in capturing novel transaction behaviors that deviate from legitimate financial activity.

4.4 Scalability and Computational Efficiency

Scalability is a crucial factor for blockchain fraud detection, as networks process millions of transactions daily. Traditional graph-based fraud detection models often struggle with processing efficiency, particularly when handling large-scale datasets. The proposed STGNN model

e-ISSN: 3079-6377 p-ISSN: 3079-6369

incorporates graph partitioning and parallelized inference techniques, improving computational efficiency while maintaining high detection accuracy.

The model achieved a 40% reduction in inference time compared to static graph-based approaches. Mini-batch processing significantly optimized memory consumption, enabling real-time transaction monitoring without excessive computational overhead. The ability to process blockchain transactions efficiently ensures that the model remains suitable for large-scale deployments, such as cryptocurrency exchanges and regulatory compliance platforms.

4.5 Limitations and Future Considerations

Despite its strong performance, the STGNN model has limitations that must be addressed for broader adoption. One key limitation is the computational cost associated with training deep graph models on extensive blockchain datasets. While inference remains efficient, training requires substantial processing resources, which could limit deployment feasibility in real-time fraud detection environments. Future research should explore optimization strategies such as federated learning and distributed training to improve scalability further.

Another challenge is model interpretability. Like other deep learning models, STGNN-based fraud detection lacks transparency in its decision-making process, making it difficult for regulators and financial analysts to understand why specific transactions are flagged as fraudulent. Future work should focus on integrating explainable AI techniques to enhance fraud detection accountability and build trust in automated security systems.

Additionally, as blockchain ecosystems evolve, cross-chain transactions and multi-layer DeFi protocols introduce new complexities in fraud detection. Future iterations of the model should incorporate multi-chain analysis capabilities to track fraudulent asset transfers across different blockchain networks, improving detection coverage and security enforcement.

5. Conclusion

This study introduced a scalable blockchain fraud detection framework based on STGNNs, addressing the limitations of traditional fraud detection methods. By modeling blockchain transactions as a structured graph with spatial and temporal dependencies, the proposed approach enables more effective identification of fraudulent activities, such as money laundering schemes, coordinated phishing attacks, and anomalous fund transfers.

The experimental results demonstrated that STGNNs outperform rule-based detection methods, supervised machine learning classifiers, and static GNN models. The model achieved an F1-score of 0.91, significantly reducing false positives while maintaining high detection accuracy. Additionally, the case study on real-world blockchain transactions validated the effectiveness of the approach in detecting large-scale fraud schemes, such as peel chain laundering and decentralized finance (DeFi) exploits. Unlike traditional methods, which rely on static transaction rules, the STGNN model dynamically learns evolving fraud patterns, allowing it to detect previously unseen illicit activities.

Scalability remains a crucial advantage of the STGNN framework, as it efficiently processes large-scale blockchain networks through graph partitioning and parallelized inference. The ability to handle high-throughput transaction streams makes the model suitable for deployment in cryptocurrency exchanges, anti-money laundering (AML) systems, and regulatory compliance

e-ISSN: 3079-6377 p-ISSN: 3079-6369

platforms. Furthermore, by incorporating reinforcement learning, the model continuously refines its fraud detection strategies, improving adaptability to emerging fraud tactics.

Despite its advantages, certain challenges must be addressed for broader adoption. The computational cost associated with training deep graph models remains a limitation, particularly in real-time fraud detection environments. Future research should explore optimization strategies such as federated learning, distributed GNN architectures, and low-latency inference techniques to improve scalability further. Additionally, model interpretability remains a concern, as deep learning-based fraud detection models often function as black-box systems. Enhancing explainability through interpretable AI techniques will be critical for improving regulatory acceptance and analyst trust in automated detection systems.

With the continuous expansion of blockchain ecosystems, including cross-chain transactions and complex DeFi protocols, fraud detection methods must evolve to handle new security threats. Future iterations of STGNN-based frameworks should incorporate multi-chain transaction analysis, enabling fraud detection across different blockchain networks and decentralized financial infrastructures. Furthermore, the integration of real-time anomaly detection with automated fraud prevention mechanisms could enhance security across digital asset platforms.

In conclusion, this study highlights the effectiveness of spatial-temporal graph-based learning in blockchain fraud detection, demonstrating superior accuracy, adaptability, and scalability over traditional fraud detection methods. As blockchain networks continue to grow, AI-driven fraud detection systems will play an increasingly vital role in maintaining the integrity of decentralized financial ecosystems.

References

[1]. Kapadiya, K., Patel, U., Gupta, R., Alshehri, M. D., Tanwar, S., Sharma, G., & Bokoro, P. N. (2022). Blockchain and AI-empowered healthcare insurance fraud detection: an analysis, architecture, and future prospects. IEEE Access, 10, 79606-79627.

[2]. Ahmed, A. A., & Alabi, O. (2024). Secure and scalable blockchain-based federated learning for cryptocurrency fraud detection: A systematic review. IEEE Access.

[3]. Bello, H. O., Idemudia, C., & Iyelolu, T. V. (2024). Integrating machine learning and blockchain: Conceptual frameworks for real-time fraud detection and prevention. World Journal of Advanced Research and Reviews, 23(1), 056-068.

[4]. Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A machine learning and blockchain based efficient fraud detection mechanism. Sensors, 22(19), 7162.

[5]. Amponsah, A. A., Adekoya, A. F., & Weyori, B. A. (2022). A novel fraud detection and prevention method for healthcare claim processing using machine learning and blockchain technology. Decision Analytics Journal, 4, 100122.

[6]. Taher, S. S., Ameen, S. Y., & Ahmed, J. A. (2024). Advanced fraud detection in blockchain transactions: An ensemble learning and explainable ai approach. Engineering, Technology & Applied Science Research, 14(1), 12822-12830.

[7]. 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.

[8]. Liang, Y., Wang, X., Wu, Y. C., Fu, H., & Zhou, M. (2023). A study on blockchain sandwich attack strategies based on mechanism design game theory. Electronics, 12(21), 4417.

e-ISSN: 3079-6377 p-ISSN: 3079-6369

[9]. Schlette, D., Caselli, M., & Pernul, G. (2021). A comparative study on cyber threat intelligence: The security incident response perspective. IEEE Communications Surveys & Tutorials, 23(4), 2525-2556.
[10]. Bhowmik, M., Chandana, T. S. S., & Rudra, B. (2021, April). Comparative study of machine learning algorithms for fraud detection in blockchain. In 2021 5th international conference on computing methodologies and communication (ICCMC) (pp. 539-541). IEEE.
[11]. Lutfiani, N., Apriani, D., Nabila, E. A., & Juniar, H. L. (2022). Academic certificate fraud detection system framework using blockchain technology. Blockchain Frontier Technology, 1(2), 55-64.
[12]. Kılıc, B., Sen, A., & Özturan, C. (2022, September). Fraud detection in blockchains using machine learning. In 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA) (pp. 214-218). IEEE.
[13]. Tripathy, N., Balabantaray, S. K., Parida, S., & Nayak, S. K. (2024). Cryptocurrency fraud detection through classification techniques. International Journal of Electrical and Computer Engineering (IJECE), 14(3), 2918-2926.
[14]. 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).
[15]. 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.
[16]. Kim, J., Nakashima, M., Fan, W., Wuthier, S., Zhou, X., Kim, I., & Chang, S. Y. (2021, May). Anomaly detection based on traffic monitoring for secure blockchain networking. In 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-9). IEEE.
[17]. Shayegan, M. J., Sabor, H. R., Uddin, M., & Chen, C. L. (2022). A collective anomaly detection technique to detect crypto wallet frauds on bitcoin network. Symmetry, 14(2), 328.
[18]. 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.
[19]. Hisham, S., Makhtar, M., & Aziz, A. A. (2022). Combining multiple classifiers using ensemble method for anomaly detection in blockchain networks: A comprehensive review. International Journal of Advanced Computer Science and Applications, 13(8).
[20]. Ofori-Boateng, D., Dominguez, I. S., Akcora, C., Kantarcioglu, M., & Gel, Y. R. (2021). Topological anomaly detection in dynamic multilayer blockchain networks. In Machine Learning and Knowledge Discovery in Databases. Research Track: European Conference, ECML PKDD 2021, Bilbao, Spain, September 13–17, 2021, Proceedings, Part I 21 (pp. 788-804). Springer International Publishing.
Mouratidis, H., Islam, S., Santos-Olmo, A., Sanchez, L. E., & Ismail, U. M. (2023). Modelling language for cyber security incident handling for critical infrastructures. Computers & Security, 128, 103139.