Dean&Francis
ISSN 2959-6157

# A Survey of Deep Learning-Based Methods for Detecting Anomalous Transactions in Blockchain

**Qiujing Fan**

Department of Management and Economics, Tianjin University, Tianjin, China
Email: fanqiujing_123@tju.edu.cn

**Abstract:**

The decentralized and anonymous nature of blockchain technology has driven the growth of the digital economy while introducing new challenges in detecting anomalous transactions. This paper systematically reviews recent advances in deep learning-based methods for identifying anomalous transactions in blockchain. It analyzes the main types of blockchain-based anomalous transactions and their risks, highlighting the limitations of traditional detection methods in handling high-dimensional, nonlinear transaction data. Furthermore, this survey provides a detailed introduction to six major categories of deep learning approaches: graph neural network-based methods, which effectively model transaction network topologies; autoencoder-based methods that identify anomalies through reconstruction errors; generative adversarial networks that mitigate data imbalance issues; attention mechanisms capable of capturing critical transaction features; temporal models suited for analyzing transaction timing patterns; and multi-feature fusion methods that enhance detection comprehensiveness. For each type of method, this paper summarizes the representative research achievements and their performance, and discusses the key challenges faced by current research and proposes future research directions.

**Keywords:** Blockchain, Anomalous transaction detection, Deep learning, Graph neural network

## 1. Introduction

Blockchain represents a distributed ledger system established on cryptographic principles. It has four fundamental features: decentralized architecture, data immutability, transaction transparency, and participant anonymity [1]. These features bring broad application prospects to blockchain, but also pose new challenges for anomaly transaction detection. There are various manifestations of abnormal transactions in blockchain systems, including large-value transactions, high-frequency transactions, and abnormal transaction patterns. These abnormal transactions may hide illegal activities such as money laundering,

ISSN 2959-6157

terrorist financing, market manipulation, and pose a serious threat to the blockchain ecosystem and user assets.

There are three traditional methods for anomaly detection: statistical analysis techniques, rule-based systems, and machine learning algorithms. The statistical approach detects deviations by analyzing the numerical characteristics of transaction data, including measures of central tendency and dispersion metrics. Rule-based systems work by comparing transaction instances against a predefined set of suspicious pattern indicators. Machine learning solutions employ either supervised classification or unsupervised clustering algorithms to identify potential anomalies. However, when applied in the blockchain context, these traditional methodologies exhibit notable limitations. However, blockchain transaction data has high-dimensional and nonlinear characteristics, and traditional methods are difficult to effectively extract complex features from it. What's more, the anonymity of blockchain makes transaction behavior difficult to track and correlate. With the increasing complexity of attack methods, traditional methods are unable to cope with new abnormal trading patterns.

As an advanced subfield of machine learning, deep learning provides new ideas for anomaly detection in blockchain environments. Deep learning models can automatically learn high-level features from raw transaction data, capture complex patterns and abnormal behaviors in the data, As a result, deep learning implementations have shown substantial improvements in both the accuracy and effectiveness of anomaly detection systems.

This study systematically reviews the research on blockchain anomaly transaction detection based on deep learning both domestically and internationally, providing reference for researchers in related fields. The main contributions of this study are summarized as follows:

· The study focuses on six mainstream deep learning approaches, discussing their principles, applicable scenarios, and innovative applications in blockchain anomaly detection, including graph neural networks (GNNs), autoencoders (AEs), generative adversarial networks (GANs), attention mechanisms, temporal models, and multi-feature fusion methods.

· For each method, a comparative analysis is conducted to objectively evaluate detection performance, computational efficiency, and the advantages and disadvantages of real-world deployment.

· The study systematically summarizes key scientific challenges and technical bottlenecks in the field, proposing forward-looking solutions and future research directions, which helps provide theoretical foundations and technical guidance for promoting the secure and orderly development of the blockchain ecosystem.

## 2. Evaluation Metrics for Deep Anomaly Detection

The research community has established a set of widely recognized evaluation criteria, principally comprising accuracy, recall, precision, and the F1-score. The evaluation system is based on the construction of four core elements of confusion matrix: true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN).

· TP quantifies instances where anomalous samples are correctly identified.

· TN enumerates cases where normal samples are properly classified.

· FP represents the misclassification of normal samples as anomalies.

· FN accounts for anomalous samples that evade detection.

1) Accuracy

Accuracy measures the proportion of correctly predicted samples (both normal and anomalous) among all samples. The calculation formula is:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

2) Recall

Recall evaluates the model's ability to identify true anomalies, representing the true positive rate. It is calculated as the ratio of correctly detected anomalies to all actual anomalies:

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

3) Precision

Precision focuses on the proportion of true anomalies among samples predicted as anomalous, emphasizing the reduction of FPs. The calculation formula is:

$$Precision = \frac{TP}{TP + FP} \tag{3}$$

In scenarios where false alarms are costly (e.g., anomaly detection systems, network monitoring), high precision is critical, indicating high reliability of reported anomalies.

4) F1-Score

The F1-score is the harmonic mean of precision and recall, balancing the impact of FPs and FNs. It provides a single comprehensive performance metric when trade-offs between recall and precision are necessary. The calculation formula is:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{4}$$

Identify applicable sponsor/s here. (sponsors)

5) False Positive Rate (FPR)
FPR measures the proportion of normal samples incorrectly classified as anomalies. The calculation formula is:

$$FPR = \frac{FP}{TN + FP} \tag{5}$$

6) False Rejection Rate (FRR)
FRR measures the proportion of true anomalous samples incorrectly classified as normal. The calculation formula is:

$$FRR = \frac{FN}{TP + FN} \tag{6}$$

## 3. Deep Learning-based Anomalous Transaction Detection Methods

A. Graph Neural Network-based Anomalous Transaction Detection
The blockchain transaction network is inherently a complex graph structure where nodes may represent addresses or transactions, and edges can denote fund transfer relationships between addresses. Graph neural network-based anomalous transaction detection methods employ deep learning models such as Graph Convolutional Networks (GCN) and Graph Neural Network (GNN) to model address relationships and transaction network structures, thereby identifying anomalous transaction behaviors.
Patel et al. [2] presented an innovative framework leveraging Graph Neural Network (GNN) architectures for the identification of suspicious transactions within the Ethereum network. They collected the external transaction data on Ethereum, manually marked the abnormal transactions, and then extracted the features. Experimental results show that the model is superior to the traditional method based on machine learning in terms of accuracy and F1 score.
In order to tackle the issue of class imbalance in graph data, Chang et al. [3] put forward an enhanced version of the Graph Attention Network (GAT) named SGAT-BC. This proposed method incorporates a subtree attention mechanism to improve the performance of GAT. It integrates two ensemble learning strategies: self-aggregation (Bagging) and cost-sensitive boosting (CAT). Through experimental validation on four real-world blockchain transaction datasets, the results demonstrate that the performance of SGAT-BC is significantly better than the existing baseline model.
Lin et al. [4] introduced GMM-CCT, a graph-based multi-model fusion approach, aimed at detecting anomalous cross-chain transactions. GMM-CCT combines an LR-XGBoost-GCN-mixed model and applies Node2vec to map graph nodes into low-dimensional vector spaces. The experimental results show that gmmcct achieves equivalent performance with the most advanced single chain scheme. The accuracy rate of normal label is 82%, and the recall rate is 89%.
B. Autoencoder-based Anomalous Transaction Detection
An autoencoder is an unsupervised learning model which makes use of an encoder-decoder framework to derive low-dimensional representations of data. In the realm of anomaly transaction detection, autoencoder-based approaches first learn the feature representations of normal transactions. Subsequently, they identify anomalies by capitalizing on the reconstruction errors that occur when processing data, which serve as indicators of deviations from the learned normal patterns.
Wu et al. [5] proposed a blockchain anomaly detection method based on the Stacked Autoencoder (SAE) , which can improve the model's representation ability. They used deep neural networks composed of multiple autoencoder layers to learn high-level feature representations of transaction data and then identified anomalies through reconstruction errors. This methodology obtained a high degree of detection precision on Ethereum blockchain datasets. Specifically in the context of processing complex transaction patterns, it showed superior performance compared to traditional autoencoder techniques.
Scicchitano et al. [6] proposed a deep autoencoder ensemble approach for detecting anomalous behaviors in blockchain. According to the research of Huang et al. [7], they defined the snapshot integrated codec model for identifying the anomaly of timing data, and realized anomaly detection by calculating the anomaly score of each instance of timing data.

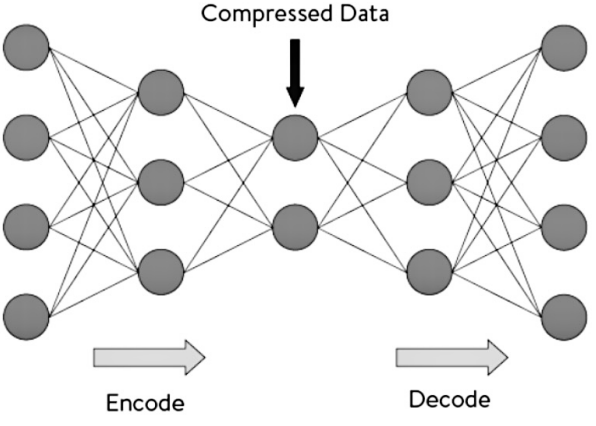


**Figure 1. Autoencoders architecture**

C. Generative Adversarial Network-based Anomalous Transaction Detection
A Generative Adversarial Network (GAN) is a deep - learning model that consists of two key components: a generator and a discriminator. It acquires the ability to understand data distributions by engaging in adversarial

ISSN 2959-6157

training processes. The abnormal transaction detection approach based on generative adversarial networks leverages GAN to generate synthetic data for expanding the training dataset, or to identify abnormal transactions by learning the normal data distribution.

In the context of blockchain anomaly detection, where challenges such as imbalanced samples, small and incomplete data sets are prevalent, Xiong et al. [8] put forward a novel detection model named GANNomaly. This model innovatively combines the generative adversarial network (GAN) and autoencoder technologies. It consists of three core modules: data generation, encoding, and detection. When it comes to identifying abnormal transactions, GANNomaly demonstrates significantly better performance compared to traditional methods. It effectively reduces the false alarm rate and enhances both the accuracy and efficiency of detection.

Li et al. [9] proposed a CPS multivariate temporal anomaly detection method based on GAN-LSTM. This model captures system interaction features through joint modeling of multi device temporal data, and integrates GAN discriminator output and generated residuals for detection, achieving high detection rate and low false alarm rate in CPS attack detection.

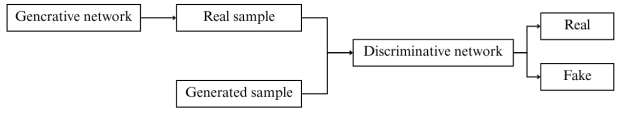


**Figure 2. Generative adversarial network structure**

D. Attention Mechanism-based Methods

Attention mechanism is a deep learning technique that improves model performance by focusing on important parts of input data. In blockchain anomaly transaction detection, attention mechanisms are used to capture important features or time steps in transaction data.

Liang Fei et al. proposed the Transformer Tam Tm model, which is applied to the malicious address detection technology involved in the transaction flow graph of Ethereum addresses [10]. The model integrates the influencing factors of transaction amount and transaction time in the Transformer self attention mechanism, enabling the model to learn abnormal information of fund flow characteristics during the transaction process from Ethereum malicious tag addresses. The experimental results show that Transformer Tam Tm outperforms traditional detection algorithms in terms of precision, recall, and F1 metrics in the test set.

E. Time-series Model-based Anomalous Transaction Detection

Blockchain transaction data has obvious temporal characteristics, and transaction behavior often exhibits certain regularity over time. Time-series based anomaly detection methods utilize deep learning models like Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) networks to capture temporal dependencies in transaction data for identifying abnormal patterns.

Sun et al. [11] developed an LSTM-based Transaction Tree Classifier (LSTM-TC) for Bitcoin mixing detection, framing the problem as a transaction classification task. This deep learning approach for feature extraction and classification outperforms traditional rule-based methods and graph neural network algorithms, particularly in detecting novel mixing transactions. While experimental results validate its superior performance, the method remains constrained by training data annotation quality and faces limitations in feature representation when processing ultra-large transaction trees. The proposed transaction filtering solution alleviates computational burdens but may compromise some information completeness.

Tang et al. [12] introduced PeerClassifier, an attention-enhanced stacked LSTM approach that significantly improves transaction pattern classification accuracy by modeling node behavior sequences. Experiments confirm its superiority over conventional techniques, with potential for further improvement through enhanced behavior feature extraction and novel method development.

F. Multi-feature Fusion-based Anomalous Transaction Detection

Multi-feature fusion approaches have been widely adopted in blockchain anomaly detection. Researchers integrate various features including transaction amounts, frequency, and address relationships to construct comprehensive behavioral representations, thereby enhancing detection accuracy.

Zhu Huijuan et al. proposed BATDet [13], a blockchain anomaly detection model based on Residual Network (ResNet-32). This model automatically learns high-level abstract features through deep residual networks while employing a feature fusion mechanism to effectively combine these learned features with original transaction details. The design automatically filters noise and discovers cross-feature correlations, significantly improving feature representation capability. Experimental validation on the Elliptic dataset confirmed the model's effectiveness.

Li et al. [14] developed a multi-source feature fusion method for blockchain anomaly detection. They extracted diverse features including transaction amounts, timestamps, and address degrees, then utilized deep neural networks for feature fusion and learning. This approach achieved over 95% detection accuracy on Bitcoin blockchain datasets. Although this method fully utilizes various features in transaction data to improve the model's expres-

sive power, feature engineering is relatively complex.

## 4. Challenges and Future Directions

While significant progress has been made in blockchain anomalous transaction detection, it still faces many challenges and development opportunities. The main existing problems include:

· Serious data imbalance and extremely low proportion of abnormal transactions hinder model training;

· Acute scarcity of labeled data, relying on costly manual audits that struggle to cover emerging attack patterns;

· Evolving dynamic attack techniques, with existing static models showing limited capability in zero-day attack detection;

· Inadequate computational efficiency and scalability, posing challenges for real-time detection with massive transaction volumes;

· Conflict between privacy preservation and compliance requirements, as detection processes may infringe on user privacy.

In the future, research should prioritize the following directions to address these challenges:

· Developing novel deep learning architectures, such as dynamic graph neural networks and spatio-temporal Transformers, to better adapt to blockchain data characteristics;

· Exploring self-supervised and incremental learning techniques to reduce dependency on labeled data and enable continuous learning capabilities;

· Investigating multimodal data fusion methods that integrate on-chain and off-chain data for more comprehensive detection systems;

· Enhancing model interpretability through attention visualization and other techniques to improve detection credibility;

· Building cross-chain collaborative detection frameworks to counter increasingly sophisticated cross-platform attacks.

With the rapid advancement of blockchain technology, anomaly detection methods must continuously innovate. In the future, research should balance detection accuracy and computational efficiency, take into account privacy protection and compliance requirements, and strengthen the cooperation between academia and industry to jointly promote the development of this field in a more intelligent and efficient direction.

## 5. Conclusion

Deep anomaly detection on blockchain is becoming a key field, which is very important for protecting and preventing network attacks in this environment, because deep learning methods have proved their effectiveness in this field. This paper systematically reviews the detection methods based on deep learning, and analyzes and compares the advantages and limitations of various methods. Although existing research demonstrates excellent performance in metrics such as accuracy and recall, significant challenges remain—including data imbalance, adaptability to evolving attacks, and computational efficiency.

Moving forward, research should prioritize exploring novel architecture designs, self-supervised learning, multimodal information fusion, and enhanced model interpretability. These efforts will drive the field toward more efficient and intelligent solutions, ensuring robust security for blockchain applications.

## References

[1] Tama, B.A., Kweka, B.J., Park, Y., & Rhee, K.H. (2017). A critical review of blockchain and its current applications. In: 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), 109-113.

[2] Patel, V., Pan, L., Rajasegarar, S. (2020). Graph Deep Learning Based Anomaly Detection in Ethereum Blockchain Network. In: Kutyłowski, M., Zhang, J., Chen, C. (Eds.), Network and System Security. NSS 2020. Lecture Notes in Computer Science(), vol 12570. Springer, Cham. pp. 132–148.

[3] Chang, Z., Cai, Y., Liu, X. F., et al. (2025). Anomalous Node Detection in Blockchain Networks Based on Graph Neural Networks. Sensors, 25(1), 1.

[4] Lin, Y., Jiang, P., & Zhu, L. (2025). Cross-chain Abnormal Transaction Detection via Graph-based Multi-model Fusion. In: Proceedings of the 6th ACM International Symposium on Blockchain and Secure Critical Infrastructure, BSCI 2024. New York. pp. 1-9.

[5] Wu, Z., Liu, J., Wu, J., et al. (2023) TRacer: Scalable Graph-Based Transaction Tracing for Account-Based Blockchain Trading Systems. IEEE Transactions on Information Forensics and Security, 18: 2609-2621.

[6] Scicchitano, F., Liguori, A., Guarascio, M., et al. (2020) Deep autoencoder ensembles for anomaly detection on blockchain. In: International Symposium on Methodologies for Intelligent Systems. Springer, Berlin. pp. 448-456.

[7] Huang, G., Li, Y., Pleiss, G., Liu, Z., et al. (2017). Snapshot ensembles: train 1, get m for free. arXiv e-prints.

[8] Xiong, A., Qiao, C., Li, W., et al. (2025). Blockchain abnormal transaction detection method based on generative adversarial network and autoencoder. High-Confidence Computing, in press.

[9] Li, D., Chen, D., Goh, J., et al. (2018) Anomaly detection with generative adversarial networks for multivariate time series. In: the 7th International Workshop on Big Data, Streams

ISSN 2959-6157

and Heterogeneous Source Mining: Algorithms, Systems, Programming Models and Applications on the ACM Knowledge Discovery and Data Mining conference. London.

[10] Liang, F., Wang, Y.J., Wang, Q., et al. (2025) Malicious address detection technology in Ethereum based on Transformer and transaction information fusion. Network Security Technology and Applications, 3: 55-59.

[11] Sun, X., Yang, T. & Hu, B. (2022) LSTM-TC: Bitcoin coin mixing detection method with a high recall. Applied Intelligence, 52: 780–793.

[12] Tang, H., Jiao, Y., Huang, B., et al. (2018) Learning to Classify Blockchain Peers According to Their Behavior Sequences. IEEE Access, 6: 71208-71215.

[13] Zhu, H.J., Chen, J.F., Li, Z.Y., et al. (2021) Blockchain abnormal transaction detection method based on multi-feature adaptive fusion. Journal of Communications, 42: 41-50.

[14] Lin, W. (2022) Detection of Abnormal Transactions in Blockchain Based on Multi Feature Fusion. Netinfo Security, 22: 24-30.

[15] Perales Gómez, Á.L., Fernández Maimó, L., Huertas Celdrán, A., et al. (2024) A Review of SUSAN: A Deep Learning based anomaly detection framework for sustainable industry. In: 9th National Conference on Cybersecurity Research (JNIC). Sevilla. pp. 454-455.