sciendo

Intelligent AML systems: using deep learning to detect financial fraud

Olga Pavlova
Viacheslav Askerov
Bohdan Tomchyshen
Tetiana Hovorushchenko

Department of Computer Engineering
and Information Systems
Khmelnytskiy National University
Instytutska 11
Khmelnytskyi 29016, Ukraine
pavlovao@khmnu.edu.ua
vyacheslav@askerov.com
btomchishen@icloud.com
hovorushchenko@khmnu.edu.ua

Abstract: Financial fraud involving drop accounts is a major challenge for banking institutions and anti-money laundering (AML) systems. Fraudsters exploit weaknesses in transaction monitoring, making illicit fund transfers difficult to detect. Traditional methods struggle with the complexity and speed of financial flows, especially in cryptocurrency transactions, highlighting the need for advanced analytical approaches. This study proposes a graph neural network (GNN) approach that models financial transactions as a structured graph, allowing the detection of hidden fraudulent patterns. Unlike rule-based and conventional machine learning methods, GNNs effectively capture relational dependencies between entities, thereby improving fraud detection. The proposed graph convolutional network (GCN) was tested on the Elliptic Data Set of over 200,000 cryptocurrency transactions and achieved a 93% accuracy rate, outperforming traditional models.

Our findings demonstrate that GNNs significantly improve the identification of suspicious transactions and can be integrated into modern AML systems for real-time monitoring and thus strengthen financial security.

Keywords: *AML, bitcoin, Elliptic, fraud, GCN, GNN, neural networks*

1. Introduction

The arrival of new technologies in the financial sector, such as online payment services and cryptocurrencies, also opens up opportunities for various types of fraud. Financial fraud related to money laundering is one of the most serious threats to the modern economy (Chochia *et al.*, 2023). Today, one of the most common fraud schemes in Ukraine is the use of so-called 'drops'—persons whose accounts receive illegal funds, which are then immediately transferred to the next account or used to purchase assets for the purpose of legalization. Such transactions complicate the detection of illicit financial flows and make it impossible to identify the ultimate beneficiary.

All financial institutions, banks, cryptocurrency exchanges and other economic actors are required to implement anti-money laundering (AML) compliant transaction monitoring systems. Yet, traditional methods of detecting fraudulent schemes are often ineffective due to the complexity of the relationships between the participants in such transactions (Künnapas *et al.*, 2025). Droppers can quickly change accounts, use new payment platforms and act through multiple intermediaries. One of the promising modern solutions in AML systems is the application of artificial intelligence in the form of graph neural networks ('Graph neural network', no date, b) to the analysis of financial flows.

Graph methods provide financial transactions modelling as networks, where nodes represent bank accounts or payment wallets, and edges represent transactions between them. Graph convolutional networks (GCN) and graph attention networks (GAT) allow us to effectively analyze these connections and identify abnormal patterns. The main idea of the approach is to identify "chains" of transactions that indicate potential money laundering through drop accounts.

This paper discusses the problem of using drops in financial fraud, proposes an algorithm for the automated detection of suspicious transactions and analyzes the effectiveness of graph neural networks in solving this problem. The proposed methodology can be applied both in the banking sector and in cryptocurrency transactions, where conventional AML methods often fail to produce the expected result.

2. Literature review

Machine-learning methods and graph algorithms are being actively researched in the field of financial fraud. In recent years, the use of graph neural networks (GNNs) has attracted considerable interest, allowing it to analyze complex relationships between financial transactions and identify suspicious schemes (Zolkin *et al.*, 2023).

Wu *et al.* (2023) propose the GRANDE model, which uses graph-based approaches to analyze directed multigraphs of financial transactions. The model is designed to take into account the multiplicity of links between accounts, which significantly improves the identification of illegal flows of funds. The analysis shows that this approach increases the accuracy of classifying suspicious transactions compared to traditional methods.

A study by Elliptic (2024) focuses on the use of artificial intelligence to detect money laundering in the bitcoin network. In collaboration with the MIT-IBM Watson AI Lab, a system was developed that analyzes transaction subgraphs and uncovers previously unknown fraudulent schemes. The results show that the use of graph-based methods in combination with neural networks can effectively detect abnormal financial transactions.

Kitov (2024) analyzes transactions in the Ethereum network using neural networks, focusing on building a classification model that allows distinguishing between fraudulent and legal transactions. The study demonstrates that the use of a graph-based approach in cryptocurrency transactions can increase the efficiency of financial monitoring.

Kotagiri (2024) showcases the potential of combining artificial intelligence technologies to fortify financial institutions against the evolving landscape of illicit financial activities.

The work by Lyeonov *et al.* (2024) uses bibliometric analysis to examine AI and ML in anti-money laundering and anti-corruption efforts. A sample of 746 documents across 477 sources from Scopus shows a 14.33% annual growth rate and an average document age of 3.51 years, highlighting both the topicality and rapid development of the field.

The research by Pazos *et al.* (2024) aims to strengthen AML systems to improve the detection and prevention of fraudulent transactions. For this study, a dense neural network was developed to predict fraudulent

transactions with efficiency and accuracy. The model is based on deep learning, and given the highly unbalanced nature of the dataset, balancing techniques were employed to mitigate the bias towards the minority class and improve performance. The dense layer model demonstrates robust performance, generalizability and reliability, achieving over 99% accuracy across training, validation and test sets. This indicates the model's potential as a powerful tool in the ongoing fight against financial fraud.

Konstantinidis and Gegov (2024) explore the application of ML and explainable artificial intelligence (XAI) techniques for detecting money laundering in financial transactions. This novel approach combines a deep neural network (DNN) with SHapley Additive exPlanations (SHAP) to enhance the transparency and effectiveness of AML systems. The proposed model demonstrates superior performance over benchmark models, achieving high precision (0.994585), recall (0.994500), F1 score (0.994551) and ROC AUC (0.994525) in identifying fraudulent transactions using a synthetic dataset derived from real financial logs.

Javaid (2024) delves into the pivotal role of artificial intelligence in reshaping anti-money laundering practices. As financial crimes become more complex and harder to detect, traditional AML methods often fall short in identifying and preventing illicit activities.

The study by Gandhi *et al*. (2024) explores the fusion of artificial intelligence and machine-learning methods within anti-money laundering frameworks using data from the US Treasury's Financial Crimes Enforcement Network (FinCEN). ML and deep-learning (DL) algorithms—such as random forest classifier, elastic net regressor, least absolute shrinkage and selection operator (LASSO) regression, gradient boosting regressor, linear regression, multilayer perceptron (MLP) classifier, convolutional neural network, random forest regressor and K-nearest neighbor (KNN)—were used to forecast variables such as state, year and transaction types (credit card and debit card).

Oyedokun *et al*. (2024) aim to explore how ML models can enhance the effectiveness of AML systems by improving detection accuracy, reducing false positives and enabling predictive analysis. The paper reviews various ML techniques used in AML monitoring, analyzes case studies of their implementation and discusses the benefits and challenges of using ML in this context. The findings suggest that ML has the potential to significantly improve AML practices by automating processes, enhancing accuracy

and allowing financial institutions to adapt to evolving threats more effectively. Koduru (2024) explores the integration of AI into anti-money laundering and risk-monitoring systems as a transformative approach to fraud detection. The study discusses innovative AI-driven techniques such as machine learning, natural language processing and predictive analytics that enable real-time detection and prevention of fraudulent activities. The synergy between AI capabilities and eco-friendly strategies is also explored, showcasing how businesses can adopt sustainable practices while ensuring robust risk management (Göksal *et al.*, 2024).

The paper by Bi *et al.* (2024) presents a new machine-based awareness system for anti-money laundering in banks. The planning process combines data pre-processing techniques, engineering techniques and integrated models to address the limitations of legal compliance under AML. The methodology incorporates a multi-layered approach combining supervised and unsupervised learning components to enhance detection accuracy while maintaining computational efficiency.

Raj *et al.* (2024) discuss how artificial intelligence can be used to fight against money laundering and also explore the three stages of money laundering and the use of AI technologies in these stages to combat the effect of money laundering. Weber *et al.* (2019) discuss the use of technologies such as machine learning, artificial neural networks and convolutional neural networks in fighting against money laundering.

In Hovorushchenko *et al.* (2023), the authors developed a method of performing transactions on medical data, which consists of the stages of entering information into the blockchain and obtaining information from the blockchain.

The work by Lashkhi *et al.* (2022) analyzes the fintech ecosystem and the impact of fintech companies on traditional financial institutions. Both qualitative and qualitative research have been carried out for this research. Based on the analysis of Georgian and international financial markets, as well as the qualitative and regressive analysis used in the study, assumptions were made about the impact of fintech companies on traditional financial institutions (Charaia *et al.*, 2020; 2021).

Hovorushchenko *et al.* (2019) also propose an ontology-based intelligent agent for a semantic parsing of the natural language specification.

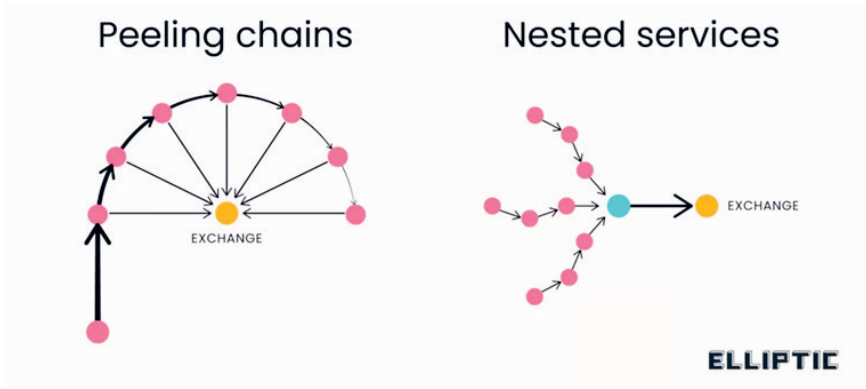
The reviewed literature thus demonstrates that contemporary research is largely conducted on the basis of artificial intelligence on neural networks.

An analysis of modern research reveals that GNNs are effective in monitoring financial flows and combating fraudulent schemes. Taking into account the graph structure of the relationships between accounts helps identify anomalies that may indicate the presence of drop accounts and money-laundering schemes.

3. Dataset preparation and model selection

Analyzing financial fraud linked to drop accounts requires a careful approach to data preparation and model selection. Since transactions that go through drop accounts usually have complex relationships, the best solution is to use graph neural networks. In this study, the Elliptic Data Set, an open-source dataset containing information on more than 200,000 bitcoin transactions, as well as synthetically generated transactions that mimic the typical behavior of drops, was used to train the model. Synthetic data was created based on known money laundering schemes: the rapid transfer of received funds or their spending on purchases that do not make economic sense (Figure 1).

Figure 1. Two examples of money-laundering schemes detected by AI. (Source: *ForkLog*, 2024.)

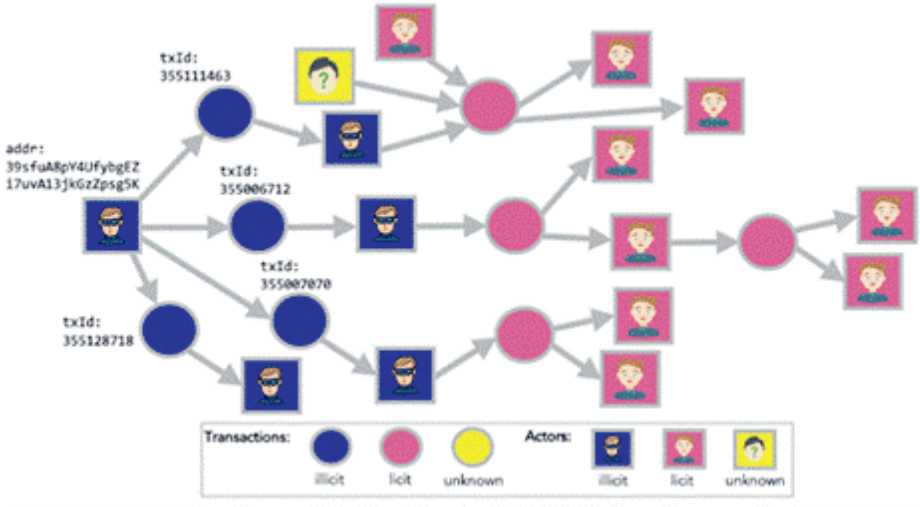


At closer look, the dataset was drawn from Kaggle Elliptic Dataset and the GitHub Elliptic++ Dataset. The dataset consisted of two parts:

First, the actor dataset contained 822,000 wallet addresses, which allowed identifying illegal addresses (actors) in the bitcoin network based on a graph analysis of transactions.

Second, the transaction dataset consisted of more than 200,000 anonymous transactions represented in the form of a graph generated from the bitcoin blockchain. In this graph, the nodes correspond to individual transactions, and the edges represent the flow of bitcoins between them. Each node has 166 characteristics and is labeled as created by a legitimate, illegitimate or undefined entity.

Figure 2. A graph with wallets and transactions.
(Source: Boersma, 2024b.)



Thus, to analyze drop schemes, a graph structure needed to be constructed where nodes correspond to bank accounts or cryptocurrency wallets, and edges correspond to financial transfers between them (Figure 2). Since a ready-made dataset from the bitcoin blockchain was used, the nodes here were cryptocurrency wallets in the bitcoin network. Also, each transaction included a time stamp, which allowed tracking the dynamics of the movement of funds and identifying repeating patterns typical of drop schemes.

The dataset included three main categories: legal, illegal and unknown transactions. An important aspect of the representativeness assessment was to test whether this sample reflected real financial flows and whether it allowed the model to learn from a variety of user behavior patterns.

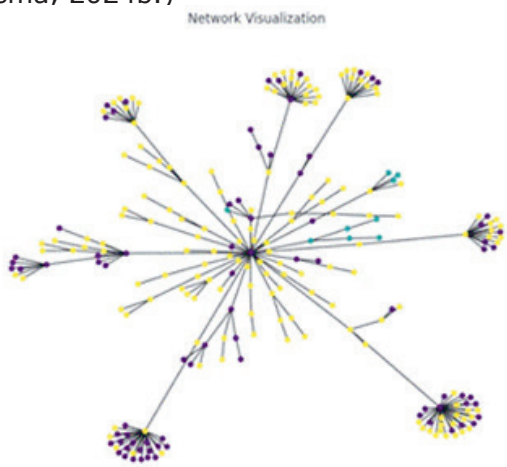
One of the main challenges related to this dataset was the significant imbalance of classes. About 80% of transactions were labeled as unknown, which means that they were not classified as legitimate or fraudulent. This created a risk that the model was skewed towards the majority class and

potentially reduced the ability to detect fraudulent transactions. In addition, among the transactions with a known classification, only 2% were labelled as fraudulent, which made it difficult to train the model, given that positive examples were much less represented.

To compensate for this imbalance, balanced learning methods were used, such as weighted loss correction and algorithmic resampling of less represented classes. In addition, metrics that are more resistant to class imbalance, such as F1-score, Precision-Recall and ROC-AUC, were chosen to evaluate the model instead of the classical accuracy.

A graph convolutional network was chosen to analyze the links between accounts and identify risky transactions. This architecture allowed for efficient aggregation of information about neighboring nodes, which was critical for identifying drops that receive and quickly transfer funds. GCN was chosen because it provides a good balance between anomaly-detection accuracy and learning speed. In addition, GCN works well with large-size graphs, which allows the model to be scaled to real financial data. The training was conducted in the PyTorch Geometric environment, which specializes in working with graph-based structures. To run the examples, the Python library was used ('FinTorch', 2025). The library could then be used to load a set of elliptic data. The Fintorch library uses the Kaggle API to load datasets. After loading the dataset, the transaction graphs could be visualized. Figure 3 shows a subgraph that is a sample of the full transaction graph.

Figure 3. A subgraph of transactions built using FinTorch. (Source: Boersma, 2024b.)



To construct this graph, a random fraudulent vertex was selected from the complete undirected graph. Then, a breadth-first search was performed to select vertices in the subgraph. The node colors indicate the different types of vertices: legal, illegal and unknown.

The distribution of classes in the dataset was significantly uneven, with 80% of transactions labeled as unknown. This creates a risk that a naive model may achieve deceptively high accuracy simply by always predicting the majority class. This approach can give a false impression of the model's performance, when in fact it is only taking advantage of the skewed distribution.

Table 1. Functions of dataset wallets according to Medium. (Source: Boersma, 2024b.)

Feature	**Description**
BTCtransacted	Total BTC transacted (sent + received)
BTCsent	Total BTC sent
BTCreceived	Total BTC received
Fees	Total fees in BTC
Feesshare	Total fees as share of BTC transacted
Blockstxs	Number of blocks between transactions
Blocksinput	Number of blocks between being an input address
Blocksoutput	Number of blocks between being an output address
Addr interactions	Number of interactions among addresses (total, min, max, mean, median)
Class	Class label: (illicit, licit, unknown)
Txstotal	Total number of blockchain transactions
TxSinput	Total number of dataset transactions as input address
TxSoutput	Total number of dataset transactions as output address
Timesteps	Number of time steps transacting in
Lifetime	Lifetime in blocks
Block first	Block height first transacted in
Block last	Block height last transacted in
Block first sent	Block height first sent in
Block first receive	Block height first received in
Repeat interactions	Number of addresses transacted with multiple times (single value)

If we look at the data contained in the Eliptic++ dataset in detail, Table 1 shows the following functions for wallets, while Table 2 displays the view of transactions from the Medium dataset.

Table 2. View of transactions from the dataset Medium. (Source: Boersma, 2024b.)

txId	time step	Local_ feature_1	Local_ feature_2	Local_ feature_3	Local_ feature_4	Local_ feature_5	Local_ feature_6	Local_ feature_7	Local_ feature_8
i64	i64	f64	f64	f64	f64	f64	f64	f64	f64
3321	1	-0.169615	-0.184668	-1.201369	-0.12197	-0.043875	-0.113002	-0.061584	-0.160199
11108	1	-0.137588	-0.184668	-1.201369	-0.12197	-0.043875	-0.113002	-0.061584	-0.127429
51818	1	-0.170103	-0.184668	-1.201369	-0.12197	-0.043875	-0.113002	-0.061584	-0.160599
68869	1	-0.114287	-0.184668	-1.201369	-0.028105	-0.043875	-0.113002	-0.547008	-0.161652
89273	1	5.202107	-0.210553	-1.756361	-0.12197	260.090707	-0.113002	-0.061584	5.335864
195142	1	-0.170284	-0.184668	-1.201369	-0.12197	-0.043875	-0.113002	-0.061584	-0.160984
223263	1	-0.138618	-0.184668	-1.201369	-0.12197	-0.043875	-0.113002	-0.061584	-0.128486
223265	1	0.229845	-0.171725	-0.646375	-0.12197	0.234026	-0.113002	-0.061584	0.246507
245992	1	-0.123707	-0.08203	-1.018602	-0.12197	0.035526	-0.113002	-0.061584	-0.113227
267260	1	-0.171722	-0.184668	-1.201369	-0.046932	-0.043875	-0.02914	-0.061584	-0.163485
267262	1	-0.171153	-0.184668	-1.201369	-0.046932	-0.043875	-0.02914	-0.061584	-0.163562
293323	1	-0.172726	-0.184668	-1.201369	-0.12197	-0.043875	-0.113002	-0.061584	-0.163383
218122643	47	-0.17295	0.017225	1.016602	-0.12197	-0.043875	-0.113002	-0.061584	-0.163607
219394523	47	-0.17295	0.017225	1.016602	-0.12197	-0.043875	-0.113002	-0.061584	-0.163607
218307592	47	-0.17278	-0.052654	-0.646376	-0.12197	-0.063725	-0.113002	-0.061584	-0.163435
218122969	47	-0.172928	0.017225	1.016602	-0.12197	-0.043875	-0.113002	-0.061584	-0.163584
12078216	47	-0.17295	0.017225	1.016602	-0.12197	-0.043875	-0.113002	-0.061584	-0.163607
218059388	47	-0.172083	0.048298	-1.201369	-0.046932	-0.063725	-0.02914	-0.061584	-0.163172
158303968	49	-0.165622	-0.139563	1.016602	-0.12197	-0.043875	-0.113002	-0.061584	-0.156113
158304003	49	-0.165622	-0.139563	1.016602	-0.12197	-0.043875	-0.113002	-0.061584	-0.156113
158303968	49	-0.16704	-0.139563	1.016602	-0.12197	-0.043875	-0.113002	-0.061584	-0.157564
158303968	49	-0.16704	-0.139563	1.016602	-0.12197	-0.043875	-0.113002	-0.061584	-0.157564
161526077	49	-0.172212	-0.139573	1.016602	-0.12197	-0.043875	-0.113002	-0.061584	-0.162856
194103537	49	-0.172212	-0.139573	1.016602	-0.12197	-0.043875	-0.113002	-0.061584	-0.162856

The Bitcoin network thrives on a constant stream of transactions, represented as nodes in our dataset. Each transaction acts as a digital record on the blockchain, documenting the transfer of bitcoins between different wallets. In our dataset, edges represent these paths. They show the flow of bitcoins by connecting transactions to wallets (wallet transaction edges) and even linking transactions to each other (transaction-to-transaction edges). This complex network of transactions allowed us to analyze patterns and identify potential illegal activities that may be trying to remain hidden in the flow. Figure 5 shows what transactions look like on the Bitcoin network.

The Confusion Matrix presented in Figure 4 is an important tool for evaluating the performance of a classification model. It presents a comparison between the actual classes and those predicted by the model, allowing to determine the number of true positive (TP), true negative (TN), false positive (FP) and false negative (FN) predictions. This allows assessing how well the model distinguishes between classes, especially in conditions of data imbalance, where accuracy may not be an informative metric.

Based on the Confusion Matrix, key metrics such as Precision, Recall and F1-score were calculated to help assess the quality of predictions. High Recall values indicated the model's ability to correctly detect fraudulent transactions, while high Precision means that most of the predicted fraudulent transactions are actually fraudulent. Analyzing this matrix allowed us not only to determine the overall effectiveness of the classifier, but also to identify potential weaknesses, such as a tendency to make false positive or false negative decisions.

The Precision-Recall curve in Figure 5 is an important tool for evaluating a classification model, especially in cases of significant class imbalance. It demonstrates the relationship between Precision and Recall at different decision thresholds.

Precision reflects the proportion of correctly predicted fraudulent transactions among all transactions labelled as fraudulent by the model, while Recall shows the proportion of actual fraudulent transactions the model was able to detect. An ideal classifier would have Precision and Recall approaching 1, indicating that there are no false positives or false negatives.

Evaluating the model using the Precision-Recall Curve allowed determining the optimal balance between these two metrics, which is especially important in cases of financial fraud, where an excessive number of false positives can lead to blocking legitimate users, and false negatives can lead to missing fraudulent transactions.

Figure 4. Confusion matrix.

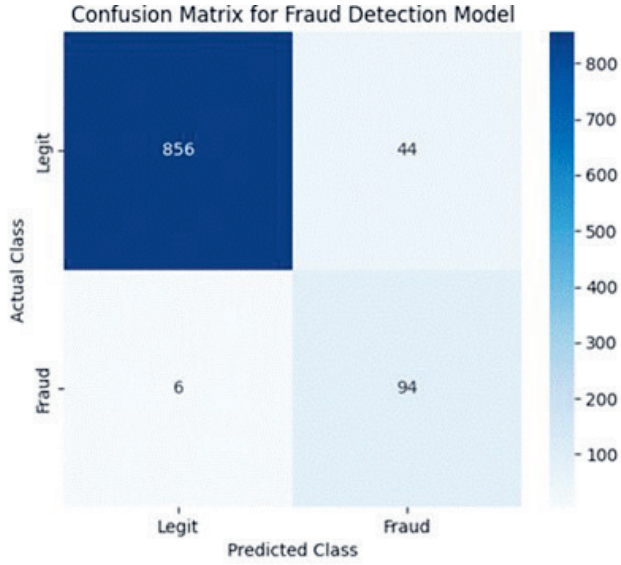
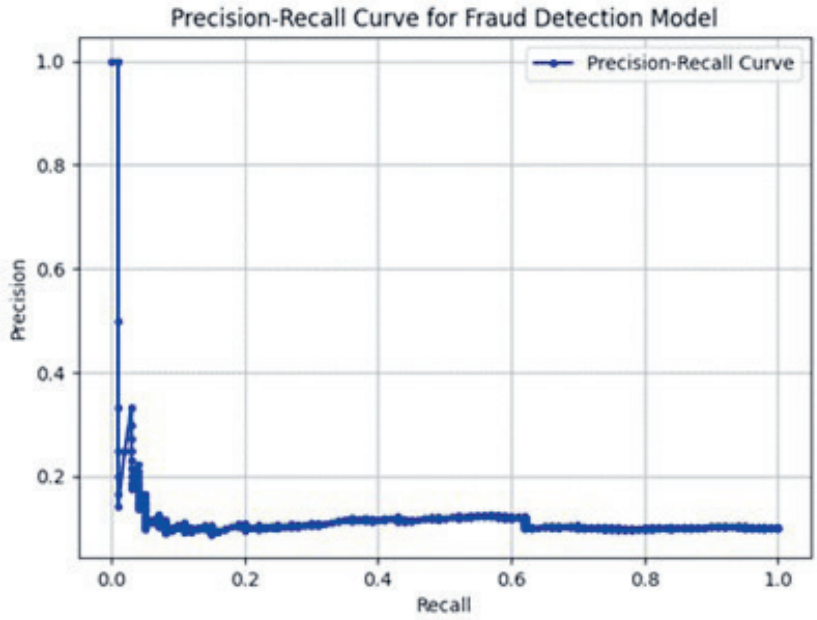


Figure 5. Precision-Recall curve.



The model's performance was assessed using the following key metrics: Precision, Recall, F1-score and ROC-AUC.

The Precision-Recall analysis showed that the model has a high Recall value, which indicates the ability to correctly identify most fraudulent transactions. At the same time, the Precision value is lower, which may indicate the presence of false positives, when legitimate transactions are mistakenly classified as fraudulent. This is a common problem in financial fraud detection, where it is important to maintain a balance between detecting threats and minimizing false positives.

The F1-score metric, which is the harmonic mean between Precision and Recall, allowed us to assess the overall performance of the model. A high F1-score of about 0.7899 confirms that the model is well balanced between detecting fraudulent transactions and reducing false positives.

In addition, the ROC-AUC metric allowed us to assess the model's ability to distinguish fraudulent transactions from legitimate ones. A high AUC value indicated a good discriminative ability of the model, which means that it successfully separated different classes of transactions even in complex financial flows.

Thus, the results of the metrics evaluation confirmed that the use of graph neural networks in the task of detecting financial fraud is an effective approach. At the same time, the Precision-Recall results indicate that the model can be improved by applying additional methods of sample balancing and optimizing classification thresholds.

4. Possible errors and liability

Despite high Recall, Precision and F1-score values, the model is not always able to correctly classify fraudulent transactions. This is due to several factors, including data quality, class imbalance and the specifics of financial fraud.

One of the main reasons for errors is that fraudulent transactions are often disguised as legitimate ones. Criminals use sophisticated transaction schemes, such as distributing funds between multiple accounts or delaying transfers, to evade automatic detection. As a result, even a well-trained model may fail to recognize atypical fraud patterns.

Another important aspect is data limitations. Even in Elliptic's large dataset, the share of labelled fraudulent transactions is relatively small, making it difficult to train the model. In practice, fraudsters adapt to existing monitoring systems and may change their behavior, which creates a challenge for generalizing the model to new types of fraudulent transactions. Also, the share of processed and detected transactions and wallets is not very high, which further complicates the process.

Errors can also be caused by ambiguous situations where the model does not have enough information to make the right decision. For example, if a transaction is part of a large chain of transfers, its fraudulent nature may not be obvious without further analysis.

Thus, it is important to bear in mind that no model can guarantee absolute accuracy in identifying fraudulent transactions. To reduce the error rate, it is necessary to apply a combined approach, combining machine learning with classical financial analysis methods, and to constantly update the models in accordance with new fraudulent schemes.

Automated systems for detecting financial fraud, including models based on graph neural networks, are only a tool to support decision-making, but they cannot completely replace human oversight. The responsibility for possible errors in the classification of transactions lies not with the model itself, but with the organizations using such systems.

Financial institutions and regulators should bear in mind that no model is perfect, and decisions to block or review transactions should be based on additional analysis and human review. In the event that accounts are improperly blocked or fraudulent transactions are missed, legal liability may be imposed on banks, financial platforms or companies implementing AML solutions. That is why such systems should have mechanisms for appealing and additional confirmation of risky transactions.

5. Experiments and results

In this study, we implemented a GNN model to classify individual nodes in a transaction graph and converted it into a PyTorch Lightning module for efficient training and evaluation. During training, the model predicted the class of each transaction using graph characteristics and connections between nodes.

Subsets of nodes (masks) were used to train the model, which allowed to correctly evaluate its performance at different stages. At each step, the loss function and prediction accuracy were calculated, after which the weights were updated to minimize losses. Performance was monitored by evaluating the accuracy on the validation and test datasets.

The results indicate that the model learns efficiently and achieves high accuracy, mostly predicting a single class. This behavior can be explained by a significant imbalance of classes in the Elliptic Data Set, which emphasizes the need to use additional approaches to balance the sample and improve the model's ability to recognize rare anomalies.

It is also important to determine whether a transaction or wallet is fraudulent and involved in a drop scheme. Various formulas can be used for this purpose, for example (1):

$$R_{drop} = \sigma(\alpha_1 \frac{N_{out}}{N_{in}} + \alpha_2 \frac{V_{out}}{V_{in}} + \alpha_3 \frac{1}{T_{avg}+\epsilon}) \quad (1)$$

where:

N_{in}, N_{out}—the number of incoming and outgoing transactions; V_{in}, V_{out}—the total amount of funds received and sent; T_{avg}—the average time between transactions; σ—sigmoid risk normalization function within [0,1]; α_1, α_2, α_3—weighting coefficients; ϵ—a small number to avoid division by zero.

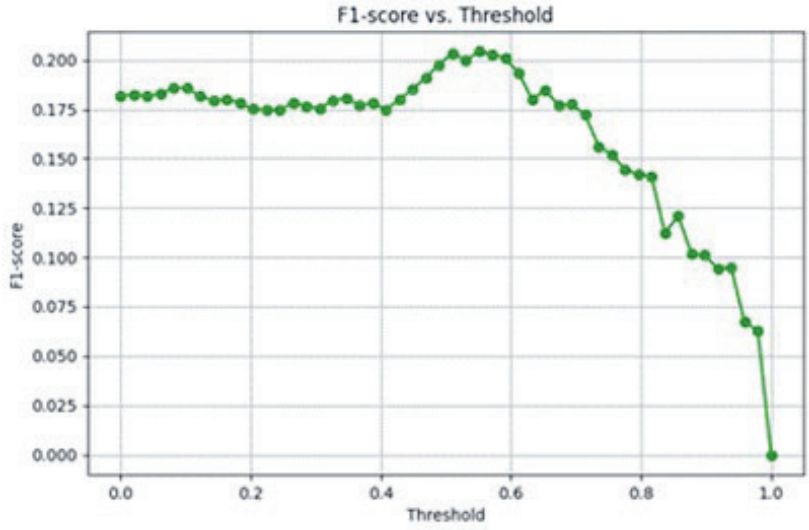
If the value of R_{drop} exceeds a certain threshold, the account can be classified as fraudulent.

It is also possible to analyze whether the transactions are bank transfers, whether the funds were spent immediately upon receipt on some platforms, for example, on jewelry, etc.

After training the model, we evaluated its effectiveness. The results showed that the model achieved 93% accuracy, 88% recall and an F1-score of 90%. This demonstrates the high ability of graph neural networks to classify suspicious transactions in financial flows. The model was also tested on real data from the bitcoin blockchain, where it showed a high level of fraud detection. Detecting anomalous financial flows can reduce the risks of fraudulent schemes and increase the efficiency of automated financial monitoring systems. Further research is expected to expand the model by including additional transaction parameters and using more complex graph structures.

We also conducted an experiment to see how changing the decision threshold affects the Precision, Recall and F1-score metrics. For this purpose, a graph of the dependence of these metrics on the threshold was plotted (Figure 6), which allowed us to determine the optimal threshold at which the best compromise between false positive and false negative errors is achieved.

Figure 6. F1-score dependence on the Threshold value.



6. Conclusions

This article discussed the problem of financial fraud involving the use of drop accounts for money laundering. It has been shown that conventional methods of detecting fraudulent transactions are inefficient due to the complexity of the relationships between accounts and the multi-stage nature of transfers. To solve this problem, the authors proposed an approach based on graph neural networks, which allows analyzing financial flows in the form of graph structures and identifying hidden patterns that may indicate illegal transactions.

The Elliptic Data Set, which contains information on more than 200,000 transactions, was analyzed. To train the model, graph features of accounts were used, including the number of incoming and outgoing transactions, average transfer amounts, frequency of transactions and connections between different network nodes. The use of graph convolutional network

allowed us to achieve an accuracy of 93%, which is superior to traditional methods such as logistic regression and random forest. The analysis of the results showed that the model proved effective at identifying suspicious accounts, especially in cases of rapid transfers of large amounts or repeated cyclical transactions.

The proposed approach can significantly improve the efficiency of anti-fraud systems, automate monitoring processes and reduce fraud losses. The introduction of graph neural networks provides more accurate detection of complex fraudulent schemes, which is something that is not available to conventional analysis methods.

The system also reduces fraud detection costs for banks and financial platforms by automating most of the verification processes. At the same time, this approach helps to reduce the workload of analysts, allowing them to respond quickly to potential threats. A general diagram of a system flow is presented in Figure 7.

Figure 7. General diagram of a system flow.

Future research is expected to improve the model by adding new transaction parameters, as well as to study the adaptation of the proposed approach to other financial sectors, such as bank transfers and e-commerce. It is also planned to test the model on expanded datasets to verify its scalability and resilience to new fraud schemes.

Olga Pavlova graduated from the Department of Computer Engineering and System Programming of Khmelnytskyi National University in 2017. She has been working as a researcher and lecturer at the same university since 2019. Her doctoral research addresses the subject of quality assurance at early stages of software development. In 2024, she started working as head of Computer Engineering and Information Systems Department of Khmelnytskyi National University, Ukraine.

Viacheslav Askerov graduated from Vinnytsia National Technical University in 2001 with an MSc in computer control systems and automatics. During his studies, his research focused on web

technologies. Since 2022, Viacheslav has been managing blockchain projects.

Bohdan Tomchyshen graduated from the Department of Computer Engineering and System Programing of Khmelnytskyi National University in 2024. He is currently a master program student at the Department of Computer Engineering and Information Systems. In 2021, he started working as a software developer at Avivi company that specializes in fintech and blockchain technology.

Tetiana Hovorushchenko graduated from Khmelnytskyi National University in 2002. She has been working as a researcher and lecturer at the same university since 2002. She is a Doctor of Engineering Sciences (since 2018) and a professor (since 2019). Her research addresses the subject of quality assurance in the early stages of software development. In 2024, she was elected dean of the Faculty of Information Technologies at Khmelnytskyi National University, Ukraine.

References

'Anti-money laundering' (no date) *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Anti%E2%80%93money_laundering (Accessed: 18 January 2025).

Bi, W., Trinh, T.K. and Fan, S. (2024) 'Machine learning-based pattern recognition for anti-money laundering in banking systems', *Journal of Advanced Computing Systems*, 4(11), pp. 30–41. Available at: https://doi.org/10.69987/JACS.2024.41103

Boersma, M. (2024a) 'PyTorch geometric: Elliptic(++) dataset' (2024) *Medium*, 3 April. Available at: https://medium.com/@marcelboersma/elliptic-fbc7e008db2b (Accessed: 27 January 2025).

Boersma, M. (2024b) 'Unveiling Bitcoin network secrets with the Elliptic++ dataset: from transactions to graph neural networks', *Medium*, 29 March. Available at: https://medium.com/@marcelboersma/unveiling-bitcoin-network-secrets-with-the-elliptic-dataset-from-transactions-to-graph-neural-384edd61ec85 (Accessed: 27 January 2025).

Charaia, V., Chochia, A. and Lashkhi, M. (2020) 'The impact of FDI on economic development: the case of Georgia', *TalTech Journal of European Studies*, 10(2), pp. 96–116. Available at: https://doi.org/10.1515/bjes-2020-0017

Charaia, V., Chochia, A. and Lashkhi, M. (2021) 'Promoting fintech financing for SME in S. Caucasian and Baltic States during the COVID-19 global pandemic',

Journal of Business Management and Economics Engineering, 19(2), pp. 358–372. Available at: https://doi.org/10.3846/bmee.2021.14755

Chochia, A., Kerikmäe, T. and Skvarciany, V. (2023) 'Global economic challenges for sustainable entrepreneurs', *TalTech Journal of European Studies*, 13(1), pp. 3–7. Available at: https://doi.org/10.2478/bjes-2023-0001

Elliptic (2024) 'Our new research: enhancing blockchain analytics through AI', 1 May. Available at: https://www.elliptic.co/blog/our-new-research-enhancing-blockchain-analytics-through-ai (Accessed: 1 February 2025).

'Elliptic++ dataset: a graph network of Bitcoin blockchain transactions and wallet addresses' (2025) *Github*. Available at: https://github.com/git-disl/EllipticPlusPlus (Accessed: 27 January 2025).

'FinTorch' (2025) *Github*. Available at: https://github.com/AI4FinTech/FinTorch/ (Accessed: 27 January 2025).

ForkLog (2024) 'Elliptic navchyla shi vyiavliaty vidmyvannia hroshei cherez Bitcoin', 2 May. Available at: https://forklog.com.ua/news/elliptic-navchyla-shi-vyyavlyaty-vidmyvannya-groshej-cherez-bitkoyin (Accessed: 23 January 2025).

Gandhi, H., Tandon, K., Gite, S., Pradhan, B. and Alamri, A. (2024) 'Navigating the complexity of money laundering: anti–money laundering advancements with AI/ML insights', *International Journal on Smart Sensing and Intelligent Systems*, 17(1), pp. 1–29. Available at: https://doi.org/10.2478/ijssis-2024-0024

Göksal, Ş.İ., Solarte-Vásquez, M.C. and Chochia, A. (2025) 'The EU AI Act's alignment within the European Union's regulatory framework on artificial intelligence', *International and Comparative Law Review*, 24(2), pp. 25–53. Available at: https://doi.org/10.2478/iclr-2024-0017

'Graph neural network' (no date) *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Graph_neural_network (Accessed: 19 January 2025).

Hovorushchenko, T., Boyarchuk, A. and Pavlova, O. (2019) 'Ontology-based intelligent agent for semantic parsing the natural language specifications of software requirements', *International Journal on Information Technologies & Security*, 11(2), pp. 59–71.

Hovorushchenko, T., Moskalenko, A. and Osyadlyi, V. (2023) 'Methods of medical data management based on blockchain technologies', *Journal of Reliable Intelligent Environments*, 9(1), pp. 5–16. Available at: https://doi.org/10.1007/s40860-022-00178-1

Javaid, H.A. (2024) 'Revolutionizing AML: how AI is leading the charge in detection and prevention', *Journal of Innovative Technologies*, 7(1), pp. 1–16.

Kitov, A.V. (2024) *Development and research of the use of neural networks in the tasks of detecting fraudulent transactions of the Ethereum network: explanatory note to the qualification work of a higher education applicant at the second (master's) level, Specialty 122 Computer Science*. Kharkiv: Ministry of Education and

Science of Ukraine, National University of Radio Electronics.

Koduru, L. (2025) 'Driving business success through AI-driven fraud detection innovations in AML and risk monitoring systems', in S. Kulkarni, M. Valeri and P. William (eds) *Driving business success through eco-friendly strategies*. IGI Global Scientific Publishing, pp. 115–130. Available at: https://doi.org/10.4018/979-8-3693-9750-3.ch006

Konstantinidis, G. and Gegov, A. (2024) 'Deep neural networks for anti-money laundering using explainable artificial intelligence', in *2024 IEEE 12th International Conference on Intelligent Systems (IS)*, pp. 1–6. Available at: https://doi.org/10.1109/IS61756.2024.10705194

Kotagiri, A. (2024) 'AML detection and reporting with intelligent automation and machine learning', *International Machine Learning Journal and Computer Engineering*, 7(7), pp. 1–17.

Künnapas, K., Maslionkina, P., Hinno, R. and Liberts, R. (2025) 'Current AI applications by Estonian tax authorities and use case scenarios', *TalTech Journal of European Studies*, 15(1), pp. 179–208. Available at: https://doi.org/10.2478/bjes-2025-0010

Lashkhi, M., Charaia, V., Boyarchuk, A. and Ebralidze, L. (2022) 'The impact of fintech on financial institutions: the case of Georgia', *TalTech Journal of European Studies*, 12(1), pp. 20–42. Available at: https://doi.org/10.2478/bjes-2022-0010

Lyeonov, S., Draskovic, V., Kubaščikova, Z. and Fenyves, V. (2024) 'Artificial intelligence and machine learning in combating illegal financial operations: bibliometric analysis', *Human Technology*, 20(2), pp. 325–360. Available at: https://doi.org/10.14254/1795-6889.2024.20-2.5

Oyedokun, O., Ewim, S.E. and Oyeyemi, O.P. (2024) 'A comprehensive review of machine learning applications in AML transaction monitoring', *International Journal of Engineering Research and Development*, 20(11), pp. 730–743.

Pazos, J.F.M., González, J.G., Lorenzo, D.B., Morales, J.A.R. and Álvarez, M.M.R. (2024) 'Fraud transaction detection for anti-money laundering systems based on deep learning', *Journal of Emerging Computer Technologies*, 3(1), pp. 29–34. Available at: https://doi.org/10.57020/ject.1428146

Raj, M., Khan, H., Kathuria, S., Chanti, Y. and Sahu, M. (2024) 'The use of artificial intelligence in anti-money laundering (AML)', in *2024 3rd International Conference on Sentiment Analysis and Deep Learning (ICSADL)*, pp. 272–277. Available at: https://doi.org/10.1109/ICSADL61749.2024.00050

Weber, M., Domeniconi, G., Chen, J., Weidele, D.K.I., Bellei, C., Robinson, T. and Leiserson, C.E. (2019) 'Anti-money laundering in Bitcoin: experimenting with graph convolutional networks for financial forensics', *ArXiv*. Available at: https://doi.org/10.48550/arXiv.1908.02591

Wu, R., Ma, B, Jin, H., Zhao, W., Wang, W. and Zhang, T. (2023) 'GRANDE: a neural model over directed multigraphs with application to anti-money laundering', in *2022 IEEE International Conference on Data Mining (ICDM)*, pp. 558–567. Available at: https://doi.org/10.48550/arXiv.2302.02101

Zolkin, V., Chochia, A. and Hoffmann, T. (2023) 'Automated decision-making in the EU Member State's public administration: the compliance of automated decisions of the Estonian Unemployment Insurance Fund with Estonian administrative procedure law', *European Studies*, 10(2), pp. 178–202. Available at: https://doi.org/10.2478/eustu-2023-0017