Detection of Money Laundering on Blockchain Systems Using Artificial Intelligence

Ertuğ Erdoğan, İbrahim Ethem Göze, Cedan Murat Zeynepli, Muhammed Said Soykan
E-mail: erdoganer19@itu.edu.tr goze19@itu.edu.tr zeynepl19@itu.edu.tr soykan19@itu.edu.tr

Abstract—Money laundering, a crime that causes significant economic damage, has become more complex with technological developments. The rise of blockchain technology has led to increased anonymity in financial transactions, providing new avenues for illegal activities such as money laundering. This study used artificial intelligence to detect money laundering in the blockchain network. Using the Bitcoin Transaction Graph Elliptical dataset, our approach used only fraud-free labeled data to build an autoencoder model. This strategy enabled the effective detection of illegal transactions. The resulting model exhibited commendable performance metrics with accuracy of 0.89, F1 score of 0.94, F2 score of 0.96, and ROC_AUC of 0.96. These results underscore the model's robustness in uncovering and combating illicit financial activity in the blockchain ecosystem and reinforce the technology's vital role in enhancing financial security.

Index Terms—Autoencoder, Blockchain, Money Laundering

1 Introduction

There are huge financial problems in the world today and money laundering is one of them. According to UNODC, the annual amount of money laundering is approximately 2%–5% of global GDP, making it one of the biggest threats in the world [1]. Technology develops and changes over time, people start to use new financial systems, but while new systems provide anonymity, they also become a new door for money laundering. While money laundering is such an important problem, world governments are trying to take their own precautions on this issue. Many methods, especially machine learning applications [2], [3], artificial intelligence [4], [5] and graphic-based analysis solutions [6], [7] are widely used in this regard. However, despite all these measures taken, there is one issue that has not yet found a clear solution to money laundering: cryptocurrencies. Bitcoin, the most popular cryptocurrency whose popularity is increasing day by day, is preferred by both malicious people and fraudsters who want to launder their money due to its high trade volume. Cryptocurrencies, which have become very popular in the last 10 years, have gained an important place in the money markets, with new ones constantly being added to the list. In fact, this popularity has reached such a level that the market value, which currently exceeds 2.5 trillion dollars, continues to increase day by day [8]. Behind all this development is blockchain technology, which provides convenience to people in many matters such as anonymity and security. Blockchain is, in its simplest form, a distributed database technology that operates on a peer-to-peer network, emphasizing the protection of user privacy when exchanging encrypted blocks of data. As mentioned before, since blockchain technology and cryptocurrencies have emerged in the very near past, studies on fraud and money laundering are quite limited. To date, studies on money laundering have had deficiencies in the models developed due to lack of data, which is generally due to companies not sharing their data. However, since our work is on Bitcoin, a blockchain-based system, the data will be public and easily accessible. Although there are such conveniences in our work, the number of data sets consisting of effective transaction data is quite small. This means we have limited resources to test and improve our work. Methods that studies in this field can use include manual review method, artificial intelligence or big data-based analysis. Since it would take too much time to examine transfers one by one in the manual review method, it would not be possible to examine the entire data set. For this reason, it is a very slow method that is generally used in large volume and suspicious transactions. Artificial intelligence will be a much more effective method in this regard [9]. Because the number of suspicious transactions that computers with high processing capacity can examine at the same time will naturally be higher than that of a human. In order to detect fraud and security threats in Bitcoin transfer transactions, there is a need for effective algorithms developed in this regard and an artificial intelligence that will make the necessary calculations and detect these transfer transactions. Here, making the correct suspicious transaction identification depends on the data set size, which makes choosing the right algorithm very important. For this reason, many different studies previously written in the field of money laundering were examined in order to choose the right algorithm and to have a more experienced approach to the issue of money laundering. These studies were mentioned in the related studies section. Artificial intelligence-based solutions have witnessed extremely significant developments, especially on the bitcoin transaction chart elliptical dataset. In this study, an artificial neural network model called autoencoder was used. The dataset was rigorously labeled as suspicious, non-suspicious. Despite labeled data, the study deliberately adopted an unsupervised learning approach. Specifically, an autoencoder model was built using only non-spurious data fragments. The autoencoder takes input data and tries to minimize this difference while trying to produce the same data as output. This choice was made to take advantage of the autoencoder's feature of reconstructing entries, aiming to detect anomalies in the data. The use of unsupervised learning techniques allowed examining the underlying patterns and structures in the data set in detail. Thus, it was possible to reveal internal patterns and meaningful structures of the data set that could be overlooked in a supervised approach.

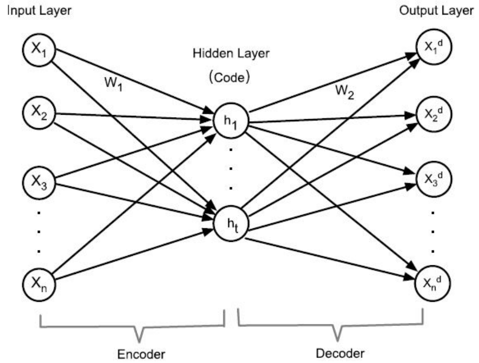

Fig. 1. Structure of AutoEncoder

Autoencoder is an unsupervised learning model that can autonomously acquire data features from a vast dataset and serve as a technique for reducing dimensionality. There are encoder and decoder layers between the input and output. As shown in [10, Fig. 2], an autoencoder comprises three distinct layers: the input layer, hidden layer, and output layer [10]. When suspicious transfer transactions are given to the trained model, the reconstruction error is higher than expected, indicating that money laundering is taking place in this transaction and intervention is required.

The aim of this article is to prove that solutions designed using artificial intelligence to detect suspected money laundering and fraud transactions in the bitcoin transfer network will have both the best accuracy and the best scores in detecting these transactions. Specifically, the study also developed existing artificial intelligence solutions with the Autoencoder model.

1.1 Our Contributions

1) Changing the proportion of data allocated as training and testing in the data set in the model used
2) Our enhancement involves implementing the Adam optimizer algorithm in the model, which optimizes the training process by dynamically adjusting learning rates for each parameter. This change significantly improves the efficiency and convergence speed of the model during training.
3) The autoencoder has undergone enhancements and refinements, resulting in the development of an improved version with advanced features and optimized functionalities

2 Related Work

Xiaobing Sun et al. [11] summarised three typical characteristics of money laundering: intensity, moderate levels of account resets and a fast-in, fast-out approach. This involves the rapid movement of significant funds from source to destination accounts with minimal intermediaries, the use of intermediate accounts as bridges with minimal balances to avoid detection, and the rapid division of illicit funds transferred through these accounts into smaller pieces. The authors focused on detecting dense blocks in tensors consisting of source, intermediate, destination accounts and other multiple features and introduced CubeFlow, a new method for detecting money laundering using merged tensors. CubeFlow not only tracks the flow of funds between source, intermediate and destination accounts, but also incorporates attributes such as transfer time to model frequent transfers made by fraudsters. They define a multi-attribute metric to identify fraudulent transfers and aim to accurately detect chains of illegal money movement in short time intervals. They developed their model with real world data.

Cheng et al. [12] introduced a novel group-aware graph neural network-based method (GAGNN) for detecting organized money laundering transactions.As illustrated in [12, Fig. 3] the solution architecture comprises three main components: a Community-centric encoder, a Group representation layer, and a Prediction network. First, the Community-centric encoder transforms transaction was recorded into graphs and encoded nodes by incorporating both topological and attribute information through graph representation learning and convolution layers. Second, the Group representation layer was generated edge representations and groups nodes associated with transactions flagged as potential money laundering. This forms a new group user transaction graph, which is then processed by the community-centric encoder to derive group representations. In order to create predictions, the Prediction network employed a joint optimization strategy that combined group detection losses, transaction classification, and node classification. Its architecture is tailored to efficiently detect organized money laundering behavior for inductive tasks involving user transaction graphs that are not well connected. The experiment was conducted with suspicious real data equivalent to 5% of all transactions, labelled with financial expert automation tools.

A brand-new technique for time-frequency analysis of financial transactions [13] was introduced by Ketenci et al.They tuned the hyperparameters by utilizing simulated annealing in conjunction with 2-D representations of the transactions generated by the Random Forest machine learning technique.They used time-frequency analysis to extract features, and they were able to achieve high accuracy with just a few characteristics. They employed a quarterly sliding time window with daily total incoming and outgoing funds as the signal granularity, and by applying the Fourier transform to each window and aggregating the results, they generated a time-frequency representation of customer transactions. Their hypothesis was that the time-frequency characteristics of everyday financial transactions would differ from suspicious ones, and they calculated 11 metrics which are,mean, variance, skewness, kurtosis, time sparsity, frequency sparcity, time-frequency sparsity, time discontiniuty, frequency discontinuity, time-frequency discontinuity, entropy, to test this. They collected data from 6,680 customers, of which 1,787 were related to suspicious activities (SAR) and 4,893 were not, analyzing 6 months of data. Six different cases are considered as input features for the model, including transaction (T) features, time-frequency (TF) features, customer properties related (CRM) features, and combinations of theseThe model was optimized using simulated annealing by altering parameters such as min-split, min-leaf, and max-depth. The objective was to maximize the Area under the Receiver Operating Characteristic curve (AUC) to enhance the model's accuracy in distinguishing true positives from false positives, with a higher AUC signifying greater accuracy.

Alkhalili et al. [14] developed a Machine Learning Component (ML-Component) for integration with existing watchlist filtering systems. ML-Component is designed in three phases: monitoring, consulting and taking action.Its goal was to investigate actions that produced false positives. Experiments were conducted with different ML algorithms and SVM showed the best performance. In order to track and update transaction decisions, the machine learning component will be deployed as an external service. The monitoring phase involves silently observing transactions, adjusting them using a portion of the model, and generating reports that compare ML Component decisions to compliance officer decisions. The consulting phase minimizes research efforts based on acceptable matches between two decisions, and human input is still needed. The action phase aims to reduce false positives and false negatives; The ML Component makes the final decision on whether to release or reject blocked transactions. The use of various data sources is taken into account when tuning the ML Component. They assessed the performance of Support Vector Machines (SVM) in two test situations, first using the default linear kernel and then switching to a polynomial kernel owing to dataset non-linearity for improved accuracy. Using stratified k-fold cross-validation, they separated the dataset into training and testing sets, making sure that distinct subsets of the same data were used in successive rounds.In order to reduce bias and increase the accuracy of the results, they employed the Min-Max scaler to standardize continuous features, making sure that feature values fell between 0 and 1.

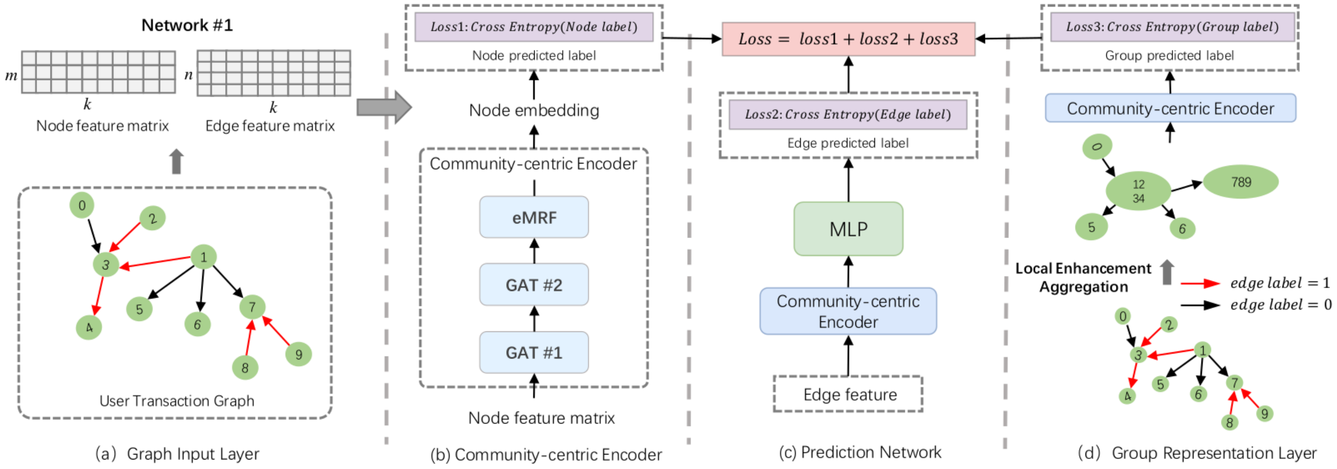

Fig. 2. The proposed model for detecting group-aware money laundering has the following structure: (a) depicts the input layer representing the user transaction graph; (b) demonstrates the architecture of the community-centric encoder; (c) presents the prediction network designed for joint optimization of nodes, edges, and group representations; and (d) details the group representation layer, which uses local enhancement operations to incorporate the outcomes.

Jensen et al. [15] explain AML terminology in the banking industry, focusing on customer risk profiling and identifying suspicious behavior. They were motivated by the Financial Action Task Force's recommendations, and the study finds knowledge gaps relating these two AML features.. Customer risk profiling relies on undisclosed characteristics and handcrafted risk indices to detect suspicious behavior while drilling down into risk factors. Among the many difficulties faced by AML are the scarcity of readily available public-domain datasets and the absence of class imbalance; however, these problems can be overcome by using techniques like data augmentation and synthetic data generation. Rather than relying solely on accuracy, it is recommended to use ROC or PR curves as evaluation metrics for AML applications. In this research by Jin et al, [16] the main focus was to detect Ponzi schemes in Ethereum transactions. The new method they introduced, called the Heterogeneous Feature Augmentation module (HFAug), collects various information about account behavior patterns and can be combined with already-available Ponzi detection methods. HFAug extracts features from a heterogeneous graph containing trade and contract call data and incorporates these features into a homogeneous graph to which Ponzi detection methods are applied. The performance of the current Ponzi detection techniques is enhanced by this addition without necessitating significant changes. The researchers ran tests to show how well HFAug performed in enhancing the performance of three different categories of Ponzi detection techniques after gathering labelled data of Ethereum Ponzi schemes.In order to evaluate the efficacy of the HFAug module, the researchers combined three distinct categories of Ponzi detection techniques—manually feature engineering, random walk-based graph embedding, and GNN-based techniques—with 191 labelled Ponzi data from various blockchain platforms. According to HFAug's extensive experiments on Ethereum datasets, these Ponzi detection techniques perform much better. They concluded that the degree of improvement achieved by HFAug is closely linked to the quality of heterogeneous information extracted from the data.

A model has been proposed to make inferences about whether addresses on the Ethereum blockchain are blacklisted or non-blacklisted [17]. The authors have pointed out that the Ethereum blockchain can be modeled as a directed graph for use in machine learning. In this regard, the transaction volume in 2021 was 11 billion dollars. One major challenge encountered during the training of the model was the numerical imbalance of classes, which was overcome using resampling techniques. Various methods were employed, including Decision Tree (DT), Random Forest (RF), Gradient Boosting (GB), K-nearest Neighbors (KNN), Support Vector Machine (SVM), and Multilayer Perceptron (MLP) classifiers. This study differs from other related works in that it includes both global and local features in the feature selection process. As a result of this study, a success rate of 97% was achieved in detecting whether an address is blacklisted.

Xu et al. [18] have demonstrated that a Bitcoin mixing service is a pool into which many users deposit their funds. These deposited funds are spread across different addresses over time to obscure their origin. In 2019, when the Binance exchange was hacked, 7,000 bitcoins were laundered through this method. This study aims to trace the path of funds laundered through Bitcoin mixing services. A new dual ensemble classification model was developed by combining their own model with a Kernel-based classification model. The Kernel-based classification model was used to identify which addresses are involved in the Bitcoin mixing service system. As a result of this study, a success rate of 99.84% was achieved in detecting whether an address is blacklisted.

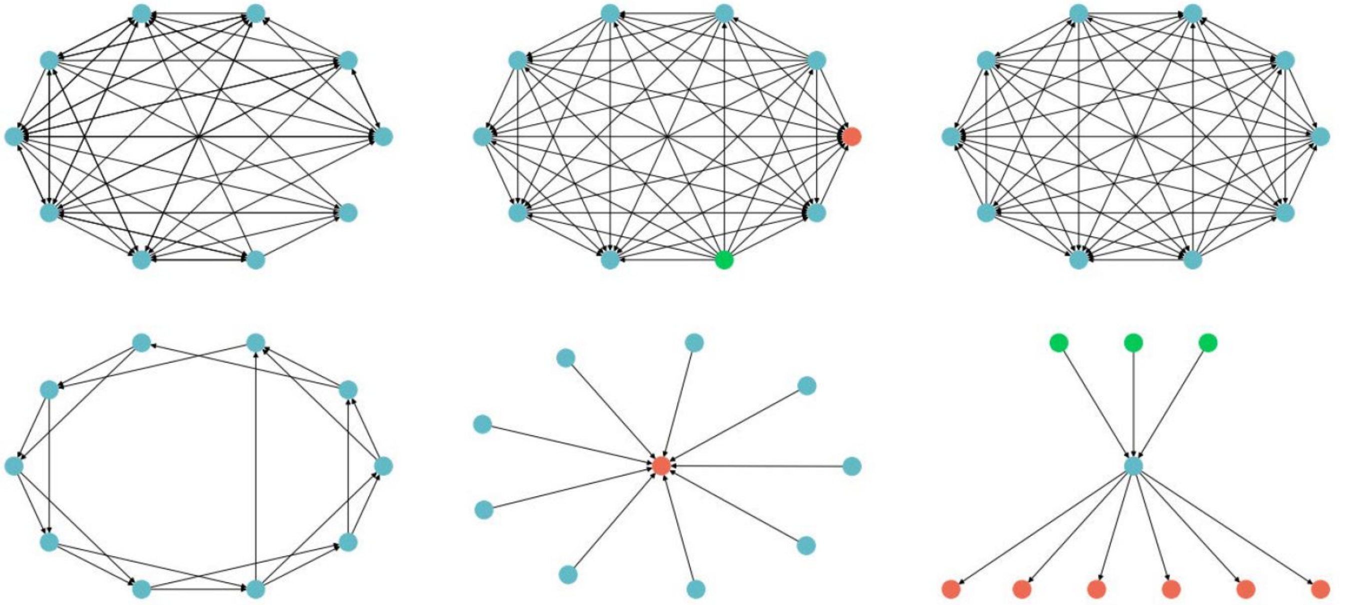

Fig. 3. Suspicious graph types

In [19], focuses on fraud detection in Bitcoin transfers within smart cities, which is a complex task. To address this complexity, the authors applied ensemble learning by combining multiple machine learning models. The machine learning model consists of two parts: the base layer and the meta layer. In the base layer, a combination of decision tree, Naive Bayes, K-nearest neighbor, and random forest models is used to derive an output from input data. These output data are then combined in the meta layer using Shapley additive explanation. ADASYN-TL is employed to balance the dataset for more effective analysis. Additionally, hyperparameter tuning is conducted to optimize the dataset for efficiency, focusing on reducing the average number of iterations to improve processing speed. Random search, Bayesian optimization, and grid search methods were utilized to select these parameters. As a result of this study, fraud detection was accurately predicted with a 97% success rate.

Yu et al. have developed an approach for detecting money laundering using Bitcoin. The research utilizes the Elliptic dataset as its primary data source in [20]. The study's main focus is on an encoder called ”transGAT.” This study is different because it is evaluating the importance of Bitcoin transactions by comparing the transaction flow to the transaction amount. Subsequently, a graph autoencoder is employed to capture all structural information from various transactions. The classification results are then extracted as the detector using the concatenated embeddings.

In [9], the authors have placed their focus on the use of explainable artificial intelligence and deep learning in the field of anti-money laundering (AML). It is worth noting that 51% of artificial intelligence studies employed in AML are considered uninterpretable, and they often rely on historical data. Since the data used is typically unlabeled, models such as deep learning and natural language processing are suitable. The study suggests that utilizing scalable graph convolutional neural networks can yield faster results, while DL-based natural language processing technology can reduce costs by as much as 30%. Additionally, AutoEncoder and PCA enable quicker and more precise anomaly detection, and using Graph Convolutional Neural Networks with Multi-Layer Perceptron yields improved outcomes.

In [21], Zhou et al. have defined Ethereum accounts from a graph classification perspective. They utilized a graph neural network called "Ethiden" to characterize user behaviors. Initially, raw Ethereum data was obtained, and this data was employed in conjunction with an Account Interaction Graph. Subsequently, a hierarchical graph attention encoder named "HGATE" was designed. This study has resulted in an improvement in account identification, with an increase of approximately 1% to 4%.

Dumitrescu et al. [22] aim to detect anomalies in transactions on both real bank data and synthetic data. They modelled the transaction data into a very simple graph; a node which represents the receiver, and an edge which represents the total amount of money transferred between those accounts. Even though valuable information lost in this process it gained some other advantages. The distinctive part of this project is that they used reduced egonets, modified some aspects of them, and combined these with random walk. Reduced egonet creates a subgraph from a particular node and add its closest neighbors. During the process it removes the irrelevant and small transactions since money laundering made in high amounts. In this newly created subgraph if there are nodes that made transactions with the nodes that are not in the subgraph, they considered to be irrelevant. The reason is if the accounts is making a lot of other activities outside of the subgraph it is likely to be a normal account. Relevant subgraph types are as illustrated in [22, Fig. 1] Another method used in the project is random walk. While traversing through the graph with Random walk, if the programs run into the same node, it creates suspicion. If this group contains many nodes, it may indicate that some money is circulating through these accounts which is a big sign.

In [23], Agarwal, Barve and Shukla mention about a model that uses machine learning to detect malicious accounts on the Ethereum blockchain. The Ethereum blockchain is a permisionless blockchain where anyone can perform transactions without requiring confirmation. The main motivation of the study is to increase the reliability and security levels of permissionless blockchains. In addition to the traditional graph features such as node degree and clustering coefficient, temporal features such as burst and attractiveness were also used. New features were obtained through feature extraction, and a high coverage of the feature space was achieved using PCA. All of these features were used in training the machine learning model. ExtraTreesClassifier, a supervised learning algorithm, played a role in detecting bad accounts. In addition to supervised techniques, some unsupervised techniques have been applied to the dataset, such as K-Means and cosine similarity. As a result, the model works with an accuracy rate of 87-88% when tested on different datasets.

Li et al. [1] discuss new money laundering methods that have emerged with the digital currency issued by CHINA. The research considers two possible scenarios: anonymous transactions and real-name transactions. The type of process used significantly affects the selection of the model to be studied. While the ChebNet-GRU model works well with anonymous transactions, traditional machine learning methods and deep learning work better with real-name transactions. ChebNet is a graph convolutional neural network model, and GRU is a variant of the LSTM model. In the named transaction scenario, the dataset is divided into 80% training and 20% testing, and in the anonymous transaction scenario, it's divided into 70% training and 30% testing. In the real name scenario, Random Forest and XGBoost models performed significantly better than the GCN model.

Wang et al. [24] states that the majority of relevant publications deal with machine learning and rule-based anti-money laundering systems. However, the volume of transaction data has an impact on machine learning-based anti-money laundering systems. Rule-based anti-money laundering systems are labor-intensive to operate and are unable to change with the evolving nature of money laundering activities. Consequently, this research develops a random walk and skip-grim model-based money laundering detection technique. This research applies the random walk algorithm on a user transfer network to produce random transfer trajectories for each user, calculating account moves within the graph based on weighted edges and neighbor extraction methods. And the project uses the Skip-Gram model by inputting the random transfer trajectories to generate feature vectors for each user, representing their transfer characteristics, aiming to identify potentially related accounts through cosine similarity based on the feature vectors obtained from the Skip-Gram model.

Wu et al. [25] indicates that work indicates that recent interest in using graph learning for financial risk management faces challenges due to transaction networks being directed multigraphs, which most existing graph neural networks struggle to handle. Anti-money laundering tasks, particularly in identifying risky transactions, aren't well-addressed by typical GNN designs focused on node-centric message passing. This paper explores neural model designs for directed multigraphs and introduces a new GNN approach that efficiently includes directional information. It proposes an improvement targeting edge-related tasks using a unique message passing system across an expanded edge-to-node dual graph, addressing the limitations of existing methods.

He et al. [26] states that machine learning methods struggle to effectively detect money laundering due to the intricate and concealed nature of fraudulent financial activities, leading to limitations in identifying complex patterns. Rule-based methods are not also good because of the complexes of money laundering as they struggle to adapt to the evolving behaviors embedded within financial transactions. An efficient subgraph isomorphism algorithm is much better due to above limitations. This algorithm is heavily based on the detect following types of subgraphs: chain, smurfing, parallel structure, star topology, incomplete reticular formation, cycle structure, complete reticular formation, tree topology.

Sun et al. [27] focuses on detecting money laundering agent accounts and suspicious behavior on a stream where money transfers between bank accounts are examined in real time. Money laundering agents attempt to conceal the origin of illegally obtained funds, and such fraudsters use clever strategies to evade detection. Therefore, it is a challenging task to accurately catch such fraudsters without supervision. Existing approaches do not consider the characteristics of these agent accounts and are not suitable for streaming settings. The paper proposes two methods, MonLAD and MonLAD-W. MonLAD is a scalable drawing algorithm that tracks the behavior of money laundering agent accounts in a transaction flow and detects anomalies using the AnoScore algorithm based on a powerful measure of statistical bias. Experiments show that MonLAD provides the best available performance on real-world data and yields explainable results. Additionally, the methods have linear scalability. By focusing on identifying and detecting the characteristic behavior of money laundering agents, the article contributes to preventing money laundering crimes and protecting the reputation of financial institutions. This work provides an effective approach for real-time money laundering detection and represents an important step towards the detection of financial crimes.

Park et al. [28] discusses that cross-border transfers of blockchain-based virtual assets (cryptocurrencies) are increasing and that these transfers create problems associated with money laundering. Due to the anonymity of the blockchain, virtual asset service providers cannot recognize senders and receivers. FATF, the international anti-money laundering organization, has introduced anti-money laundering obligations to virtual asset service providers with the anti-money laundering guide for virtual assets published in 2019. This paper proposes a customer authentication service model based on blockchain technology. The proposed service model states that there is no customer identity system review that meets all the requirements established by the FATF. The proposed model works by using a DLT system that can securely share the customer's basic credentials between VASPs. The article discusses blockchain and DLT-based virtual asset transfer and customer identity verification issues. While virtual asset service providers struggle to verify customer identities, the proposed model allows them to verify and share customer identities before transfer. The paper presents a DLT-based customer authentication service model to facilitate anti-money laundering transactions in compliance with FATF regulations. This model provides the opportunity to securely share and verify customer credentials between VASPs. In conclusion, this proposed service model provides a technical solution to customer authentication issues for cross-border virtual asset transfers and complies with international regulations.

Oad et al. [29] proposes the "Blockchain Supported Transaction Scanning" (BTS) method to combat crimes such as money laundering and terrorist financing that arise with the widespread use of bank cards. The BTS method includes rules that identify anomalies and rapid fund movements to detect abnormal transactions. These rules identify specific patterns of malicious activity in the transaction history. The BTS method also scans the transaction history and provides a list of entities that suspiciously received money. Finally, this method is applied to limit money laundering using blockchain. The proposed BTS method has been performance validated using a Java-based Spring Boot application. Experimental results show that the BTS method limits money laundering incidents by automating the transaction review process. The article also discusses the problems faced by current AML systems, highlighting the problems caused by their use of detailed rules as well as their control of limited data and demanding format requirements for data integration. The BTS method uses user-supplied data, checks the data in detail, and offers the user the ability to assign keys in the process of searching for suspicious activity. As a result, the BTS method offers an approach that uses new rules and blockchain technology to detect abnormal transactions. The performance of this approach is better than other methods and can be a valuable tool for financial institutions, governments and the banking industry looking to prevent money laundering.

Yin el al. [30] presents a graph embedding algorithm called GTN2vec, specifically designed to detect money laundering crimes on Ethereum. While emphasizing the complex structure of Ethereum, it states that various cyber crimes such as money laundering, phishing, bribery and Ponzi schemes are rapidly increasing. However, it is emphasized here that money laundering on Ethereum is significantly different from other malicious activities and it is necessary to develop a more specific money laundering detection model taking these differences into account. The article introduces a graph embedding algorithm called GTN2vec, which transforms Ethereum transaction records into a high-dimensional financial transaction graph and transforms this graph into low-dimensional vectors. This algorithm aims to extract characteristics of money laundering addresses using the gas fee and timestamp of transactions. The effectiveness of GTN2vec on a dataset created using real Ethereum data is evaluated with various classifiers such as random forest and shows a significant performance increase over other graph embedding methods. In conclusion, the paper presents a new approach to money laundering detection in Ethereum and aims to work in depth towards more features and definitions in the future.

Liu et al. [31] addresses an important issue regarding cryptocurrencies becoming a new platform for money laundering. Bitcoin mixing services, in particular, pose a significant problem in money laundering as they obscure the relationship between money senders and recipients and make it difficult to track suspicious money flows. The paper proposes an approach to solve this problem: modeling and analyzing the roles of agents in Bitcoin mixing transactions. The aim is to understand the roles and duties of agents in the money laundering process and thus provide the basis for exploring the roles of agents in real-world money laundering scenarios. The article proposes a goal-oriented modeling approach for this purpose and aims to examine the roles of agents in the Bitcoin money laundering process using the task perspective. Two different algorithms are proposed here. The first of these algorithms is to find mixing transactions. Kernel addresses appear as input in different mixing transactions. The second algorithm is proposed to find them. This is supported by an analysis using historical Bitcoin transaction data. The article details how this approach can be used to explore the roles of different agents. This work is stated to be the first example of how goal-oriented modeling can be used to represent agents in Bitcoin mixing transactions.

Zhou et al. [32] proposes an algorithm called SMLAD to detect suspicious money laundering accounts. This algorithm uses transactions initiated sequentially within a period as the analytical unit. It uses 40 statistical features to describe the properties of this processing unit. The algorithm detects suspicious transaction behavior by combining the anomaly detection method and the clustering method. Based on the algorithm results, a suspicious value (ASV) is calculated for each account. This ASV represents the average value of the top n transaction behaviors with the highest anomaly value. This is used to evaluate whether accounts are suspicious. The paper designs an interface that visually presents the algorithm results. This interface includes four coordinated visual components: algorithm results, an account's balance changes over time, transaction patterns initiated by transactions, and related raw transaction records. It uses an abacus-like design for trading pattern visualization. The article demonstrates the potential of visual analytics approaches to improve anti-money laundering processes on crypto exchanges. In the future, work is planned to improve the performance of the algorithm and the functionality of the user interface. They are also considering expanding into aspects such as creating labeled data sets and identifying different types of customers.

3 Autoencoder Usage for Money Laundering Detection

We inspire from this [33] work. On top of that by changing the ratio of test and train data we improved this work. We improved the architecture of the autoencoder by changing the node counts in the layers and moving into a new optimization method. Due to the lack of data in general we make use of the unknown data.

We have a dataset called Elliptic dataset. First of all, this dataset was balanced and the data was manipulated. Then, a model was created by processing these data with the help of an autoencoder. Finally, this model created with autoencoder was tested using this dataset with various techniques.

3.1 Autoencoder

The autoencoder used in this project is a type of artificial neural network designed specifically for unsupervised learning tasks like dimensionality reduction and feature learning. The model is divided into layers, each of which serves a specific purpose in the encoding and decoding process. The abstraction of it can be seen from Algorithm 1.

The first layer, known as the Input Layer, is precisely shaped to accommodate the feature count of the input data. This configuration ensures that the model can effectively capture the characteristics of the input data.

Moving on to the Encoder Layers, the first layer (encoded) has 100 nodes and uses the hyperbolic tangent (tanh) as its activation function. This layer also includes an activity regularizer designed to induce sparsity, which can help to prevent overfitting and encourage the learning of important features. The following encoder layer has 50 nodes and employs the rectified linear unit (ReLU) activation function, which is known for introducing non-linearity into the model.

Algorithm 1: Autoencoder Function

```
Input  : input_data
Output: autoencoder_model
Function autoencoder_function(input_data):;
    input_layer = InputLayer(Size =
      input_data_size);
    encoded = EncoderLayers(input_layer);
    decoded = DecoderLayers(encoded);
    output_layer = OutputLayer(decoded, Size =
      input_data_size);
    autoencoder_model = Model(input_layer,
      output_layer);
    autoencoder_model.compile(optimizer =
      ”adam”, loss = ”mse”);
    autoencoder_model.fit(input_data, input_data,
      batch_size = some_batch_size, epochs =
      some_number_of_epochs, shuffle = True);
    return autoencoder_model;
```

The Decoder Layers are structured similarly to the Encoder Layers, but in reverse order. The first decoder layer is made up of 50 nodes and employs the tanh activation function. The second decoder layer is made up of 100 nodes and also uses the tanh activation function. These layers collaborate to reconstruct the original input data from the encoder's compressed representation. The Output Layer, which is in charge of the final reconstruction, mirrors the shape of the Input Layer, allowing it to align with the original input data. This layer's activation function is ReLU, which is commonly used to introduce non-linearity, particularly in image reconstruction.

The Autoencoder Model is created by specifying the input and output layers, effectively defining the neural network's architecture. Finally, the model is built using the Adam optimizer, a popular optimization algorithm, with mean squared error (MSE) as the loss function of choice. MSE quantifies the difference between the model's reconstructed output and the original input data, guiding the training process to minimize this discrepancy. This comprehensive architecture serves as the foundation for a strong autoencoder model that is tailored to the characteristics of the input data.

3.2 Used Libraries

In this research, TensorFlow was utilized for the development and training of deep learning models, scikit-learn was employed for the creation and assessment of classification models, matplotlib and seaborn were applied for visualization purposes, pandas facilitated data manipulation tasks, networkx supported graphical analysis, and numpy handled numerical computations. Various performance metrics, such as f1_score, accuracy_score, confusion_matrix, roc_curve, precision_recall_curve, roc_auc_score, fbeta_score, recall_score, and average_precision_score, were computed using functions from the scikit-learn library. Additionally, features within the scikit-learn library were leveraged to construct a Support Vector Classification model through the SVC class, and dimension reduction operations were executed using TSNE.

4 Analysis of Proposed Solution

4.1 Dataset Analysis

In this study, the Bitcoin Transaction Graph Elliptic Data Set, has been utilized. A node within the graph symbolizes an individual transaction, while an edge can be interpreted as the transfer of Bitcoins from one transaction to another. The graph consists of 203,769 nodes and 234,355 edges. This dataset contains three separate sub-datasets. The dataset "elliptic_txs_classes" contains the classification labels of each bitcoin transaction.As shown in figure 4, two percent of the nodes are labeled illicit and twenty-one percent are labeled legal. Legal ones are labeled 2, illicit ones are labeled 1. The remaining transactions are declared as unknowing. The algorithm was trained by distributing the data labeled as unknown in a way that preserved the illicit-licit ratio. Autoencoder was able to achieve higher scores and accuracy when we distributed this data.

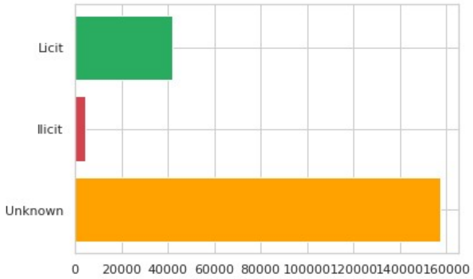

Fig. 4. Number of licit and illicit values in the dataset

The dataset "elliptic_txs_edgelist" contains a list of edges representing relationships between Bitcoin transactions. Each row in the dataset includes two transaction IDs, labeled as "txId1" and "txId2," respectively. These transaction IDs denote the direction of Bitcoin transfers. For instance, a row with "txId1" representing one transaction and "txId2" representing another indicates a Bitcoin transfer from the first transaction to the second. Thanks to this dataset, we were able to show the bitcoin money flow on a graph in our study. The "elliptic_txs_features" file represents a dataset containing features related to Bitcoin transactions. There are 166 features associated with each node. These features are numerical values expressing specific attributes of each Bitcoin transaction, such as transaction amount, input and output addresses, transaction timestamp, and transaction-related statistics. The first 94 features in the table capture local information about the transaction, including details like the time step, number of inputs/outputs, transaction fee, and average BTC amounts associated with the inputs/outputs. The remaining 72 features represent aggregated information, obtained by considering transactions one-hop backward/forward from the central node. These aggregated features encompass statistics such as maximum, minimum, standard deviation, and correlation coefficients of neighboring transactions for the same information data, providing a comprehensive view of the network's characteristics. These features have played a crucial role in developing models aimed at detecting fraudulent transactions. An autoencoder was created using the features of transactions labeled as legal. Later, mostly illegal transactions were given as input and they were determined to be illegal or not.

4.2 Environment of the Testing System

It is essential to provide details about the testing system environment, as the analysis is specific to this working setup. Different workspaces may yield varying runtimes and system outputs.

- **Central Processing Unit:** Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz
- **Graphics Processing Unit:** Onboard Intel UHD Graphics 620
- **RAM:** 8GiB DDR4
- **Hard Disk:** SanDisk Ultra II SSD 105 GB
- **Run-time:** 23 sec

4.3 SVM

SVM is a machine learning algorithm that is used for classification and regression tasks. We used it for analyzing the code and decide if it is working well or not. SVM works by determining the best hyperplane in a high-dimensional space for separating data points of different classes. Support Vector Classification (SVC) is a classification implementation of SVM. After obtaining the latent representations of the data from the autoencoder, the SVC model from the scikit-learn library is used for classification in this project. The SVC's decision function is used to compute the predicted probabilities, and the ROC curve and AUC-ROC score are then analyzed to assess the model's performance.

4.4 Rating Metrics

4.4.1 Confusion Matrix

When we input our test set into the trained autoencoder, we reached the following numbers: 5005 True Positives, 371 True Negatives, 617 False Positives, and 74 False Negatives. Our confusion matrix is as follows. Label 1 represents illicit data, while label 0 represents licit data. We found the accuracy to be 0.89. Results can be seen on Figure 5

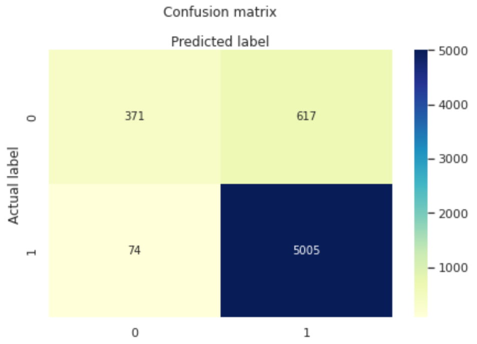

Fig. 5. Confusion Matrix

4.4.2 ROC Curve

The ROC-AUC value of 0.96, being very close to 1, indicates that the model provides high sensitivity and specificity in fraud detection. The model demonstrates a robust specificity level of 0.99, highlighting its effectiveness in conclusively identifying fraud-free transactions. However, the lower sensitivity value of 0.38 is due to the imbalance between positive and negative classes in the dataset. Results can be seen on Figure 6

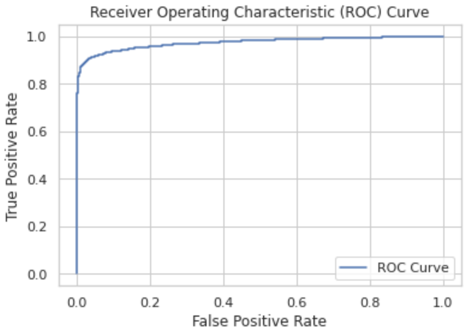

Fig. 6. ROC Curve

4.4.3 Precision-Recall Curve

Precision recall curve is a graphical representation used to measure how the system performs under different level of stringency. It is mainly used in binary classification problems which Is perfect for this case. A curve that hugs the up right corner is better since it will show under high strictness the system keeps giving precise outputs. There is also this value area under curve (AUC) for precision recall curve. The higher this value is the better it is. Results can be seen on Figure 7 PRC AUC: 0.99

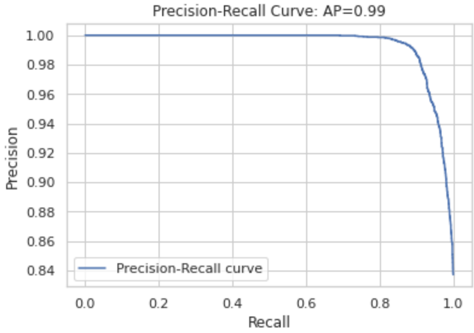

Fig. 7. Precision-Recall Curve

4.4.4 Sensitivity and Specificity

True Positive: While actual value of the datum being positive guess of the model is also positive.

False Positive: While actual value of the datum being negative guess of the model is positive.

True Positive Rate = True Positives / (True Positives + False Negatives)

False Positive Rate = False Positives / (False Positives + True Negatives)

True positive rate gives an idea about sensitivity. It can be labelled as also the ability of the model to correctly identify positive instances when they occur in the dataset. False positive rate is the rate of false instances where the model incorrectly predicts a positive outcome when the actual outcome is negative. Results can be seen on Figure 8

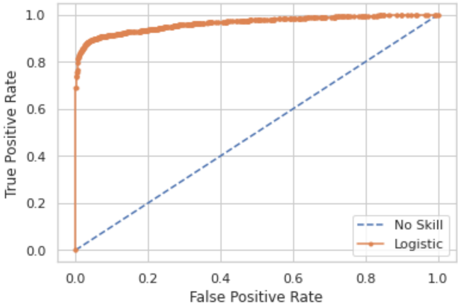

Fig. 8. Sensitivity and Specificity Curve

4.4.5 F Beta Score Test

Metric	Score
F1-score	0.94
F2-score	0.96
F_0.5 score	0.91

TABLE 1
F beta Scores

The obtained results are as follows in the table 1: F1-score: 0.94, F2-score: 0.96, F_0.5 score: 0.91. The F1-score value of 0.94 shows that the classification performance of the model is quite high. It shows that the model optimizes both precision and recall values in a balanced way. The model achieved low false positive rates in positive classifications and low false negative rates in negative classifications. Having a high F2 score is very important for us because, within the framework of our study, describing a non-fraud transaction as fraud can lead to serious losses, while low rates of fraudulent transactions as non-fraud reduce the accuracy of the model, but it does not cause grievance to customers. For this reason, we trained our model to keep the F2 score high.

5 Challenges and Limitations

5.1 Imbalanced Dataset and Lack of Fraud Data

In the elliptic dataset, the percentages of the data are as follows: %2 Fraud, %21 Non-Fraud, %77 Unknown. Since fraud activities are rare in real life, in this dataset, fraud activities are quite sparse. This is one of the biggest challenges for AI training. We overcome this problem by obtaining more data from the data labeled as unknown. Since the real proportion of fraud over non-fraud is 1/10, we divide the unknown part as 1/10 and add this to rest of the data.

5.2 Computing Power of The Environment

Training an Artificial Intelligence (AI) system is not always an easy task. The calculations involved in this process can be time-consuming. When we initially attempted to run the program on a less powerful computer, we had to wait for hours to obtain an output. Iterative testing is a significant aspect of this work, and facing limitations on the weaker system hindered our progress. Consequently, we transferred the project to a more robust computer, allowing us to continue our work with improved efficiency.

6 Conclusion

In today's world, despite all the flashy financial systems and high-tech tools such as machine learning, artificial intelligence, and chart-based analysis, money laundering still poses a huge risk to the stability of the global financial scene. Cryptocurrencies such as Bitcoin, with their hidden anonymity and large transaction volumes, have made some serious business difficult and combating dangerous financial activities even more difficult.

Because Blockchain technology, the basis of cryptocurrencies, offers both security and anonymity, integration into financial systems poses limitations for traditional fraud detection and anti-money laundering methods. The absence of adequate transactional data has limited advancement in this area, requiring the development of new approaches to overcome these barriers.

Our research primarily focused on using intelligence the autoencoder model, to identify suspicious transactions, within the Bitcoin blockchain network. One of our objectives was to enhance the accuracy of detecting money laundering activities in transactions by utilizing unsupervised learning and reliable data that is free from fraudulent elements. We categorized our three categories data into two categories; illicit, licit.

In this field of study, some neat achievements have been made. Ratios for data allocation have been adjusted, repurposing unused data by assigning new labels based on available datasets. The Adam optimization method has been employed to enhance the training process of our model, contributing to a quicker and smoother experience.

Although our study found promising strategies for improving fraud prevention in blockchain-based systems, the lack of datasets greatly hinders similar research in conventional finance systems. Therefore, companies should increase data sharing and anti-money laundering efforts.

Fighting money laundering continues to be important. It needs the teamwork of governments, overseers, technology, and banks. Studies need to focus on getting data and continue to look into the latest AI methods. These methods can help uncover and stop financial crimes in a world where finance is always changing.

6.1 Future Goals

Integration to Traditional Finance Systems: It is not possible to easily integrate these methods to banking systems due to the lack of information. It can be crucial to both train and test this model in different areas then blockchain systems. By taking into consideration the both security and privacy of the personal data banks also may share and work with the authorities to enhance money laundry detection models.

Improved Detection Algorithms: It is vital to continually improve detection algorithms to adapt to money laundering tactics in blockchain systems. Further improving our accuracy by using different AI concepts is still our main focus.

Real-Time Monitoring Solutions: It is important to move towards real-time monitoring capabilities. Developing tools and protocols that enable immediate detection and response to potential money laundering activities will be a critical step in improving the security of blockchain networks.

References

[1] Z. Li, Y. Zhang, Q. Wang, and S. Chen, ”Transactional Network Analysis and Money Laundering Behavior Identification of Central Bank Digital Currency of China,” Journal of Social Computing, 2022, pp: 219-230, doi: 10.23919/JSC.2022.0011 [Ertuğ Erdoğan]

[2] J. Domashova and N. Mikhailina, “Usage of machine learning methods for early detection of money laundering schemes,” Procedia Computer Science, vol. 190, pp. 184–192, 2021, doi: https://doi.org/10.1016/j.procs.2021.06.033. [Ertuğ Erdoğan]

[3] J. Alotibi, B. Almutanni, T. Alsubait, H. Alhakami, and A. Baz, “Money Laundering Detection using Machine Learning and Deep Learning,” International Journal of Advanced Computer Science and Applications, vol. 13, no. 10, 2022, doi: https://doi.org/10.14569/ijacsa.2022.0131087. [Ertuğ Erdoğan]

[4] D. V. Kute, B. Pradhan, N. Shukla, and A. Alamri, “Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering–A Critical Review,” IEEE Access, vol. 9, pp. 82300–82317, 2021, doi: https://doi.org/10.1109/access.2021.3086230. [İbrahim Ethem Göze]

[5] O. Garcia-Bedoya, O. Granados, and J. Cardozo Burgos, “AI against money laundering networks: the Colombian case,” Journal of Money Laundering Control, vol. ahead-of-print, no. ahead-of-print, Jun. 2020, doi: https://doi.org/10.1108/jmlc-04-2020-0033. [İbrahim Ethem Göze]

[6] Ahmad Naser Eddin et al., “Anti-Money Laundering Alert Optimization Using Machine Learning with Graphs,” arXiv (Cornell University), Dec. 2021, doi: https://doi.org/10.48550/arxiv.2112.07508. [İbrahim Ethem Göze]

[7] G.-Y. Sheu and C.-Y. Li, “On the potential of a graph attention network in money laundering detection,” Journal of Money Laundering Control, Oct. 2021, doi: https://doi.org/10.1108/jmlc-07-2021-0076. [İbrahim Ethem Göze]

[8] CoinMarketCap, “Global Charts — CoinMarketCap,” CoinMarketCap, 2023. https://coinmarketcap.com/charts/

[9] D.V. Kute, B. Pradhan, N. Shukla, and A. Alamri, ”Deep learning and explainable artificial intelligence techniques applied for detecting money laundering–a critical review,” IEEE access, doi: 10.1109/ACCESS.2021.3086230 [Ertuğ Erdoğan]

[10] P. Li, Y. Pei, and J. Li, “A comprehensive survey on design and application of autoencoder in deep learning,” Applied Soft Computing, vol. 138, p. 110176, May 2023, doi: https://doi.org/10.1016/j.asoc.2023.110176. [Ertuğ Erdoğan]

[11] Xiaobing Sun, Jiabao Zhang, Qiming Zhao, Shenghua Liu, Jinglei Chen , Ruoyu Zhuang , Huawei Shen , Xueqi Cheng, “CubeFlow: Money Laundering Detection with Coupled Tensors”, Arxiv,2021,[Cedan Murat Zeynepli]

[12] Dawei Cheng, Yujia Ye, Sheng Xiang, Zhenwei Ma, Ying Zhang and Changjun Jiang, “Anti-Money Laundering by Group-Aware Deep Graph Learning”,IEEE Xplore, 2023, [Cedan Murat Zeynepli]

[13] Utku Görkem Ketenci , Tolga Kurt , Selim Önal , Cenk Erbil , Sinan Aktürkoğlu and Hande Şerban İlhan, “A Time-Frequency Based Suspicious Activity Detection for Anti-Money Laundering”, IEEE Xplore, 2021, [Cedan Murat Zeynepli]

[14] Mohannad Alkhalili , Mahmoud H. Qutqut and Fadi Almasalha, “Investigation of Applying Machine Learning for Watch-List Filtering in Anti-Money Laundering”, IEEE Xplore, 2021, [Cedan Murat Zeynepli]

[15] Rasmus Ingemann Tuffveson Jensen and Alexandros Iosifidis, “Fighting Money Laundering With Statistics and Machine Learning”, IEEE Xplore, 2022, [Cedan Murat Zeynepli]

[16] Chengxiang Jin , Jie Jin , Jiajun Zhou , Jiajing Wu and Qi Xuan, “Heterogeneous Feature Augmentation for Ponzi Detection in Ethereum”, IEEE Xplore, 2022, [Cedan Murat Zeynepli]

[17] B. Kılıç, A. Sen and C. Özturan, ”Fraud Detection in Blockchains using Machine Learning,” 2022, pp. 214-218, doi: 10.1109/BCCA55292.2022.9922045 [Ertuğ Erdoğan]

[18] C. Xu et al., “How to Find a Bitcoin Mixer: A Dual Ensemble Model for Bitcoin Mixing Service Detection,” IEEE Internet of Things Journal, 2023, doi: 10.1109/JIOT.2023.3275158. [Ertuğ Erdoğan]

[19] N. Nayyer, N. Javaid, M. Akbar, A. Aldegheishem, N. Alrajeh, and M. Jamil, ”A New Framework for Fraud Detection in Bitcoin Transactions through Ensemble Stacking 2Model in Smart Cities,” IEEE Access, 2023, doi: 10.1109/ACCESS.2023.3308298. [İbrahim Ethem Göze]

[20] L. Yu, F. Zhang, J. Ma, L. Yang, Y. Yang, and W. Jia, “Who Are the Money Launderers? Money Laundering Detection on Blockchain via Mutual Learning-Based Graph Neural Network,” in 2023 International Joint Conference on Neural Networks (IJCNN), 2023, pp. 1-8, doi: 10.1109/IJCNN54540.2023.10191217 [İbrahim Ethem Göze]

[21] J. Zhou, C. Hu, J. Chi, J. Wu, M. Shen, and Q. Xuan, “Behavior-aware account de-anonymization on ethereum interaction graph,” IEEE Transactions on Information Forensics and Security, 2022, doi: 10.1109/TIFS.2022.3208471 [Ertuğ Erdoğan]

[22] B. Dumitrescu, A. Băltoiu, and Ş. Budula, ”Anomaly detection in graphs of bank transactions for anti money laundering applications.” IEEE Access 10, 2022, doi: 10.1109/ACCESS.2022.3170467 [İbrahim Ethem Göze]

[23] R. Agarwal, S. Barve and S. K. Shukla, “Detecting malicious accounts in permissionless blockchains using temporal graph properties,” Applied Network Science, 2021, doi: 10.1007/s41109-020-00338-3 [Ertuğ Erdoğan]

[24] Z. Wang, N. Guiqian, Z. Yan and Y. Mu, ”Detection Mechanism of Money Laundering based on Random Walk and Skip-Grim Model,” 2022 IEEE 5th International Conference on Electronic Information and Communication Technology (ICEICT), Hefei, China, 2022, pp. 444-448, doi: 10.1109/ICEICT55736.2022.9909113. [İbrahim Ethem Göze]

[25] R. Wu, B. Ma, H. Jin, W. Zhao, W. Wang and T. Zhang, ”GRANDE: a neural model over directed multigraphs with application to anti-money laundering,” 2022 IEEE International Conference on Data Mining (ICDM), Orlando, FL, USA, 2022, pp. 558-567, doi: 10.1109/ICDM54844.2022.00066. [İbrahim Ethem Göze]

[26] J. He et al., ”An Efficient Solution to Detect Common Topologies in Money Launderings Based on Coupling and Connection,” in IEEE Intelligent Systems, vol. 36, no. 1, pp. 64-74, 1 Jan.-Feb. 2021, doi: 10.1109/MIS.2021.3057590. [İbrahim Ethem Göze]

[27] Xiaobing Sun, Wenjie Feng, Shenghua Liu, Yuyang Xie, Siddharth Bhatia, Bryan Hooi, Wenhan Wang, and Xueqi Cheng. 2022. MonLAD: Money Laundering Agents Detection in Transaction Streams. In Proceedings of the Fifteenth ACM International Conference on Web Search and Data Mining (WSDM ’22). Association for Computing Machinery, New York, NY, USA, 976–986. https://doi.org/10.1145/3488560.3498418,[Muhammed Said Soykan]

[28] Park K, Youm H-Y. Proposal for Customer Identification Service Model Based on Distributed Ledger Technology to Transfer Virtual Assets. Big Data and Cognitive Computing. 2021; 5(3):31. https://doi.org/10.3390/bdcc5030031, [Muhammed Said Soykan]

[29] Oad A, Razaque A, Tolemyssov A, Alotaibi M, Alotaibi B, Zhao C. Blockchain-Enabled Transaction Scanning Method for Money Laundering Detection. Electronics. 2021; 10(15):1766. https://doi.org/10.3390/electronics10151766, [Muhammed Said Soykan]

[30] Liu J, Yin C, Wang H, Wu X, Lan D, Zhou L, Ge C. Graph Embedding-Based Money Laundering Detection for Ethereum. Electronics. 2023; 12(14):3180. https://doi.org/10.3390/electronics12143180, [Muhammed Said Soykan]

[31] Liu, Mingdong & Chen, Hu & Yan, Jiaqi. (2021). Detecting Roles of Money Laundering in Bitcoin Mixing Transactions: A Goal Modeling and Mining Framework. Frontiers in Physics. 9. 665399. 10.3389/fphy.2021.665399., [Muhammed Said Soykan]

[32] F. Zhou et al., ”Visual Analysis of Money Laundering in Cryptocurrency Exchange,” in IEEE Transactions on Computational Social Systems, doi: 10.1109/TCSS.2022.3231687., [Muhammed Said Soykan]

[33] Muhammad Gulraiz, ”AML: Machine Learning and Deep Learning - Kaggle,” Kaggle, [Online]. Available: https://www.kaggle.com/code/muhammadgulraiz/aml-machine-learning-and-deep-learning-kaggle/notebook.