2022 6th International Symposium on Computer Science and Intelligent Control (ISCSIC) | 978-1-6654-5488-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISCSIC57216.2022.00077

GAME-BC: A Graph Attention Model for Exploring Bitcoin Crime

Kai Sun
School of Computer
Beijing Information Science and Technology University
Sensing and Computational Intelligence Joint Lab
Beijing Information Science and Technology University
Beijing, China
sunkai0211@163.com

Kun Meng*
School of Computer
Beijing Information Science and Technology University
Sensing and Computational Intelligence Joint Lab
Beijing Information Science and Technology University
Beijing, China
mengkun1024@163.com

Ziqiang Zheng
School of Computer
Beijing Information Science and Technology University
Sensing and Computational Intelligence Joint Lab
Beijing Information Science and Technology University
Beijing, China
zhengzq2333@163.com

***Abstract*—Blockchain technology has been invented as a fundamental technique to the cryptocurrency Bitcoin in 2008, which is decentralized, consensus and cryptographic leger. However, due to the anonymity of the Blockchain, Bitcoin has been becoming one critical finance platform applied to transfer or hidden criminal income by offenders. Bitcoin crime refers to criminal activities which use Bitcoin as a criminal tools, criminal object or criminal settlement. Typical bitcoin crimes include online gambling, money laundering, fraud and more. To address these issues, our work aims to propose an efficient method to find transactions related with Bitcoin crime in the Bitcoin network. Which will efficiently support regulators to combat Bitcoin crimes. Through collecting and concluding kinds of Bitcoin crimes, we find several typical relation patterns among Bitcoin transactions with respect to crimes, and then construct and analysis a bitcoin criminal transaction network. At last, we study a graph neural network model with attention mechanisms to detect illegal transactions. Experimental results show that our method can achieve better classification accuracy, and has the ability to efficiently detect criminal clues and locate related illegal transactions.**

Keywords—Blockchain technology, Bitcoin crime, Graph Neural Network, Attention Mechanism, Node Classification

I. INTRODUCTION

Cryptocurrencies such as Bitcoin play an important role in the Web 3.0 and metaverse. Blockchain is a distributed ledger technology that connects blocks of data in an ordered manner. It is made impossible to tamper or forge by means of cryptography. However, due to its decentralized and highly anonymous features, users can transfer money using Bitcoin without having to provide any identifying information [1][2]. As a result, the real user is hidden behind a virtual address, which gives criminals an opportunity to take advantage of this [3].

Bitcoin crime refers to criminal activities related to the use of bitcoin as a criminal tools, criminal object or criminal settlement. Specifically, criminals are using Bitcoin as a criminal tool and object of crime when conducting illegal activities such as money laundering and fraud. In August 2012, BTCST created a Ponzi scheme to lure victims into investing in Bitcoin-related opportunities that involved 700,000 Bitcoins. On the other hand, criminals used bitcoin as a settlement method in dark web transactions and online gambling, which is typical of bitcoin crimes. in 2013, the US government shut down the dark web trading platform Silk Road[4], which involved a total of $1 billion in bitcoin. In 2017, the "WannaCry" virus broke out on the global internet. It caused a large number of files on computers to be encrypted and demanded high ransoms to be paid in Bitcoin to unlock them. Hence, it is necessary to devise a method to detect transactions on the Bitcoin network related to Bitcoin crimes. It could help regulators to track illegal transaction patterns and provide meaningful insight into the fight against illegal criminal activity [5].

Blockchain is open and transparent, and the data in Bitcoin is openly traceable. However, for reasons of protecting user privacy, the anonymity of Bitcoin makes it difficult to link blockchain data to real users. Meanwhile, since the introduction of Bitcoin in 2008, the block height has been over 750,000. All bitcoin transaction processes are publicly booked in the blockchain and the number of transactions is huge. As a result, it is difficult to detect a clear relationship between suspicious transactions and crime after many transactions. In the huge scale of bitcoin transaction data, traditional detection methods are able to identify illegal patterns. However, because it is limited by the complexity and diversity of transaction behaviors, traditional methods are difficult to detect all abnormal transactions comprehensively, and suffer from low accuracy and insufficient generalization [6][7].

Bitcoin transactions and historical information are publicly available. Although the users are anonymous, the transactions are all interconnected. We can detect transactions based on these connections and then track down illegal transactions. Bitcoin transactions are characterized by a directed graph, so it is natural that they can be analyzed from a graph perspective. Consequently, combining traditional feature engineering and graph data analysis can improve the accuracy of user transaction behavior analysis on Bitcoin [8]. However, current methods ignore global features and correlations between neighboring nodes, resulting in the loss of some important information.

Based on the above analysis, this paper proposes a bitcoin illegal transaction detection method combining graph model and attention mechanism based on bitcoin transaction graph network. We aim to achieve the detection of illegal transactions through the classification of nodes in the Bitcoin transaction graph. Our main contributions include：

1) We use a method for modelling Bitcoin network scenarios based on graph models. Mapping bitcoin data into a topological graph to achieve a complete representation of blockchain information.

2) We complete feature extraction and classification of transaction nodes by combining an attention mechanism with a graph convolutional neural network model, which improves the accuracy of the model.

978-1-6654-5488-9/22/$31.00 ©2022 IEEE
DOI 10.1109/ISCSIC57216.2022.00077

3) Finally, we adopt the method of fusing the base features of transaction nodes and network features, which effectively improves performance of the transaction node classification model.

II. Related Work

In recent years, security incidents in Bitcoin have been frequent, such as money laundering, theft, and fraudulent practices [9]. Researchers at Stanford University began focusing on money laundering in Bitcoin transactions as early as 2013, when they attempted to explore Bitcoin money laundering by clustering transaction addresses. Hirshman et al [10] first used Kmeans to cluster users in order to narrow down the target data. However, due to the lack of data labels, it was difficult to verify the effectiveness of the algorithm in tracking "bitcoin mixing" services. But they find that the transaction behaviors of some users are clearly abnormal after clustering, laying the foundation for future research into abnormal patterns in transaction data. Pham et al [11][12] use network analysis techniques to study bitcoin transactions. They first extracted user features and transaction features related to illegal behaviors patterns and used the local outlier detection algorithm Local Outlier Factor (LOF) to construct an abnormal detection model. Due to the lack of data labels, the authors used three approaches as a way to evaluate the validity of their study: checking real cases, comparing the distance to Kmeans clustering centers, and comparing the consistency of abnormal transactions with abnormal users. Based on Pham et al.'s research, to solve the problem of high computational complexity when the LOF algorithm is applied to large-scale Bitcoin transaction data, Monamo et al [13][14] proposed to use trimmed-Kmeans, an algorithm that can achieve both cluster analysis and anomaly detection, for abnormal transaction detection. In this paper, we analysis the transaction characteristics of illegal behaviors in Bitcoin and propose a classification model to classify Bitcoin transactions.

Graph neural networks have been applied in many fields and it can perform multiple tasks such as node classification, node relationship prediction, network similarity, etc. Weber et al [15][16] did an exploration of graph convolutional networks for detecting illegal transactions in the Bitcoin network. They mapped bitcoin data into a graph network and transformed the clustering problem of users and transactions into a classification problem of nodes in the graph. Based on this, they applied the Graph Convolutional Network (GCN) method to detect illegal transaction nodes, but did not achieve good results. Alarab et al [17][18] improved on the classical graph convolutional network. They proposed to connect the node embedding obtained from the graph convolution layer with a single hidden layer obtained from a linear transformation of the node feature matrix, introducing the idea of feature fusion for the first time in deep learning. In 2021, Chen et al [19] used publicly available Bitcoin data to collect theft events in it and captured behavioral features and some basic network features in terms of feature extraction. They used five supervised learning methods such as Support Vector Machine (SVM) and three unsupervised learning methods such as LOF to detect frequent bitcoin thefts. Based on this, we explore the mining of richer features related to illegal behaviors in the Bitcoin graph network using interaction information.

III. Data, Feature And Methods

A. Bitcoin Data

The data in bitcoin is stored on the blockchain in the form of a distributed ledger, and the raw data of the blockchain is stored in the form of data files on the full nodes of the blockchain network. These data files constitute the basis of the blockchain, and are also the most effective way to obtain block and transaction data for blockchain data analysis. An innovative aspect of this paper is to map bitcoin data into a graph structure. We first parse and integrate the raw data. Then valid information is extracted and blocks of information that are not relevant to the transaction are eliminated. Finally, the transaction graph is constructed according to the relationship that the output of the previous transaction is the input of the next transaction.

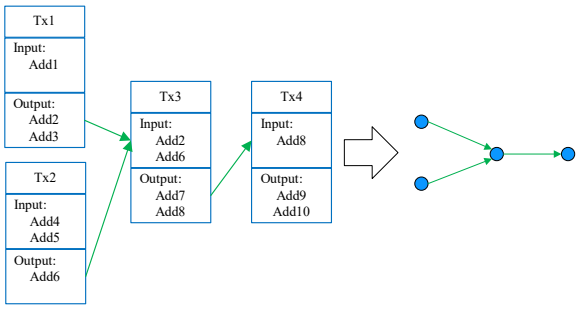

Fig. 1. Bitcoin trading graph construction relationship

The graph consists of nodes and edges, so as shown in Fig.1, the nodes of the graph in this paper represent transactions and the edges represent the flow of bitcoins between transactions. Different bitcoin crimes are expressed in different ways in the bitcoin transaction graph. Criminals usually make a number of transactions when bitcoin laundering, which is reflected in the transaction graph where multiple clusters of nodes appear. This has important implications for the analysis of characterization efforts.

B. Feature Construction

Different illicit transactions generally have different behavioral characteristics. For example, in money laundering transactions, the bitcoin addresses involved in the transaction are active for a short period of time and the average number of input and output addresses for the whole transaction is usually high. At the same time, criminals will often use many small transactions to increase the concealment of their money laundering behavior. For theft transactions, criminals often have a large number of wallet addresses, and the average number of input and output amounts between transaction addresses is roughly equal. Therefore, one of our main tasks is to filter out the more influential features based on the features provided by the Elliptic dataset. We filtered the features based on the Pearson product-moment correlation coefficient and the feature dispersion perspective. The aim of this work is to remove features with high correlation and dispersion, thereby reducing the feature dimensionality in order to increase the accuracy of the training.

C. Detecting Methods

Our proposed approach is shown in Fig.2 and is divided into two main modules: an attention layer and a graph feature convolution layer.

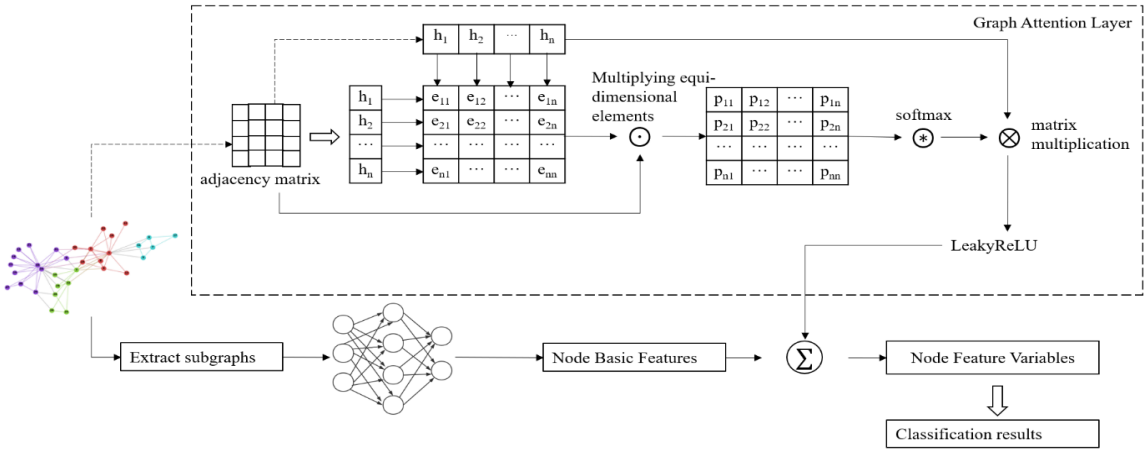

Fig. 2. Model framework diagram

The overall flow of the model is as follows: first, the classifier model takes as input the feature information matrix of the bitcoin transaction and the graph information matrix of the bitcoin transaction consisting of the transaction relationships. By optimizing the classifier model for "illegal and legal" classification, the intermediate features are used as the output. This process can be interpreted as increasing the correlation between intermediate features and abnormal illegal transactions. The aim is to solve the problem of extracting transaction graph features related to illegal behavior and to optimize the computational cost. Subsequently, the extracted transaction graph features are stitched with the feature information of the transactions themselves. The new feature vector obtained is used as the input to the classifier, and the final classification results for the illegal and legal classes are obtained. Our proposed method attempts to solve the problem of effective use of graph information in the detection of illegal transaction behavior, while attempting to improve the detection accuracy of the model.

The advantages of the attention mechanism approach in the Bitcoin transaction graph are as follows: The graph attention mechanism is a strategy that uses self-attention to compute the hidden features of each node in the graph by distributing attention values according to the importance of neighboring transaction nodes. It is flexible, efficient and portable in the generation of embedding vectors for bitcoin transaction nodes.

In this method, the Elliptic dataset contains the Bitcoin transaction graph $G = (N, E)$, where N represents the set of transaction nodes and E represents the set of edges in the graph. As shown in Equation (1) below, the input to the attention model is the set of features h of the transaction nodes, each dimension represents the feature vector matrix of a node, and the output is the updated node embedding matrix h'.

$$h = \{\vec{h_1}, \vec{h_2}, \vec{h_3} \ldots \vec{h_N}\}, \vec{h_1} \in \mathbb{R}^F \tag{1}$$

The convolutional layer is similar to the feedforward layer in that the output of each layer represents a new set of node feature vectors polymerized by an attention mechanism. To achieve the transformation of feature dimensions a weight matrix $\mathrm{W} \in \mathbb{R}^{F' \times F}$ needs to be trained, where the attentional machine value $\alpha: \mathbb{R}^{F'} \times \mathbb{R}^{F'} \rightarrow \mathbb{R}$ is introduced for self-attention, where the attentional correlation coefficient is expressed as Equation (2), which represents the importance metric of node j to node i.

$$e_{ij} = a(W\vec{h'}, W\vec{h'_j}) \tag{2}$$

The complete attention mechanism is expressed as Equation (3), where $\mathcal{N}i$ represents all neighboring nodes of node i :

$$\alpha_{ij} = \frac{\exp(\text{ LeakyReLU } (\vec{\mathbf{a}}^T[\vec{\mathbf{W}\mathbf{h}_i} \| \vec{\mathbf{W}h_j}]))}{\sum_{k \in \mathcal{N}_i} \exp(\text{LeakyReLU } (\vec{\mathbf{a}}^T[\vec{\mathbf{W}_i} \| \vec{\mathbf{W}_k}]))} \tag{3}$$

In addition, we propose a fusion feature extraction method. The process of node feature extraction for the Bitcoin transaction graph is shown in Fig.3 below. First, the blue module process is to extract the graph features of each node. After four attention convolution layers, a node embedding vector with 64-dimensional feature information is passed. Then self-attention weighting is performed to obtain the node graph feature vector. Based on the connection relationship between nodes, all node feature vectors are superimposed and summed to obtain node aggregation features. The feature aggregation method is chosen as a superposition summation rather than a stitching. This is to deal with the problem of the number of nodes in the graph varying from scene to scene using a defined network structure, and also to preserve information on the number of nodes. The nodes' aggregated graph feature vectors are stitched together with the nodes' own feature vectors (red module) to obtain the initial 128-dimensional fused feature vector. Again, weighted by the self-attentive network, the final fused feature vector of transaction nodes with dimension 128 is obtained.

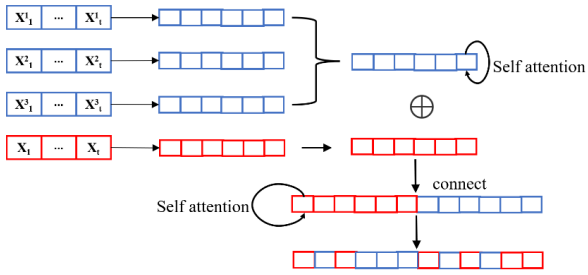

Fig. 3. Schematic diagram of the feature fusion process

IV. Experiments and Results

A. The Elliptic Dataset

In this experiment, we chose Elliptic which provides a dataset of bitcoin with tagging. The Elliptic dataset is tagged with legal transaction entity nodes and illegal transaction entity nodes. Illegal transaction entity nodes are transacting with money laundering organizations, Ponzi schemes, ransomware, telecoms fraud, etc. The Elliptic dataset has 203769 transaction nodes and 234355 directed bitcoin transaction streams. Of these, about 2% (4545) transactions were marked as illegal, 21% (42019) transactions were marked as legal, and the rest were marked as unknown. In addition to this, the dataset was divided into 49 time steps.

The Elliptic dataset provides information on the data at 49 time steps, each of which can be processed into a graph structured data. The nodes in the graph structured data are each transactional entity and there are 166 dimensional features on each node. The first 94 dimensional features are the features that exist on the nodes themselves, and the other 72-dimensional features are the features obtained by aggregating the relational nodes. The edge relationship between nodes represents the existence of a transactional relationship between nodes. Each node has its own label, and there are 3 types of labels, namely illegal, legal and unknown.

B. Experimental Setup

The data from the Elliptic dataset is divided into positive and negative samples. The negative samples were defined as illegally labelled transaction nodes and the positive samples as legally labelled samples. The training and test sets were divided in the ratio of 7:3, where the first 34 time steps were the training data and the last 15 time steps were the test data. After removing the unlabeled node samples, the total number of node samples in the training set was 29896, of which 3668 were illegal transaction nodes. The total number of node samples in the test set was 16,670, of which 1,083 were illegal transaction nodes.

For the experimental model setup, the Adam optimizer was used for training, with 650 rounds of iterative training. The learning rate was set at 0.005 and the dropout rate at 0.6 after iterative adjustment. 35 time steps of data were used for training and 14 subsequent time steps were used for validation evaluation. The hidden layer feature dimensions were set to 100 and 22, and the input data were subjected to batch gradient descent in multiple continuous time step windows in each round. The transaction data contained within each time-step window differed, but were largely maintained at an average level. Cross entropy is used here as the loss function due to the extremely uneven distribution of the samples' own labels.

In order to explore the optimal structure of an attention-based graph neural network model for detecting illegal trading behavior in the Bitcoin network, we analyzed the effect of different model structures on detection effectiveness. We first try to use skip connections in the structure, and try different graph-based attention models for the neural network, as well as try to adjust the hyperparameters used in the training. Finally, we evaluate the impact of the number of intermediate node embeddings and the number of training iterations for the training set, the validation set and for accuracy.

C. Results and Discussion

The final results on the test set are shown in Fig.4. The attention model proposed in this paper outperforms both the GCN model and the MLP+GCN model in terms of accuracy, recall and the overall evaluation metric F1. Moreover, it improved 13.6 and 2.2 percentage points in F1 score and accuracy rate respectively compared with the GCN model and MLP+GCN model.

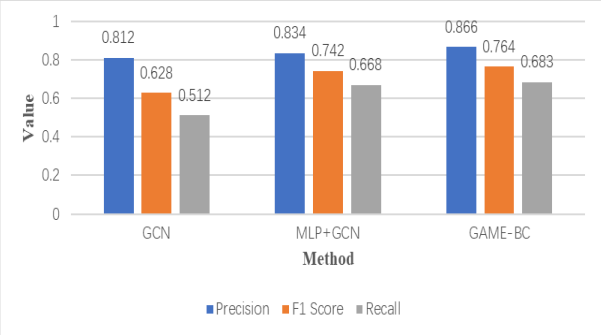

Fig. 4. Experimental results

It can also be seen from Fig.5 that the training and validation loss curves do not fluctuate significantly during the training process, and the model converges stably and is controllable overall. The validation set dynamically adjusts the hyperparameters during the training process, effectively avoiding the occurrence of overfitting and underfitting. This demonstrates that the attention mechanism is able to distribute different weights to neighboring nodes depending on their characteristics, which reflects the influence of certain important nodes and is consistent with our intuition in reality. In addition, with the introduction of the attention mechanism, the computation of the embedding of new transaction nodes is only related to the nodes neighboring on the shared edge, without the need to obtain information about the whole transaction graph. Above all, it is more friendly to the computational and memory resources needed to carry out the experiment.

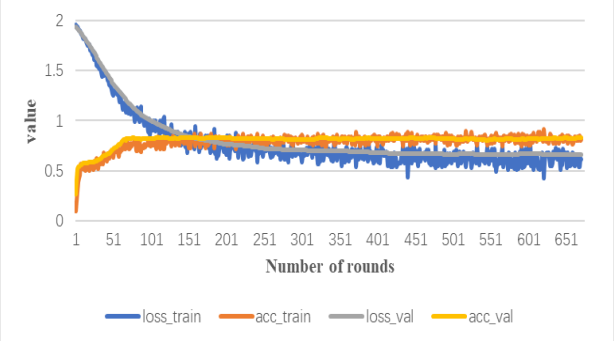

Fig. 5. Training effect graph

V. Conclusions

We propose a model based on the attention mechanism to detect illegal transactions in the Bitcoin transaction network. Compared to GCN, the attention mechanism does not rely on spectral theory, which allows it to be used as an inductive model, meaning that the full graph nodes do not have to be predicted. And to prevent the feature information of the nodes themselves from being overwhelmed by neighboring nodes, the concept of feature fusion is introduced in the attention

layer. Experimental results show that our proposed attention mechanism combined with graph neural networks significantly improves the performance of traditional graph neural network models applied only.

Bitcoin detection by using graph structured data is highly dependent on the quality of the graph structure. For the Bitcoin network as a whole, the dataset we used is small and suffers from class imbalance. In future work, we consider applying larger bitcoin graph structure datasets to detection and try to solve the class imbalance problem for the dataset. The optimization of graph convolutional networks in combination with other models will also be further explored.

REFERENCES

[1] Alabdulwahhab F A. “Web 3.0: the decentralized web blockchain networks and protocol innovation,” 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), IEEE, 2018, pp.1-4.

[2] Passinsky, Asya. "Should Bitcoin be classified as money?" Journal of Social Ontology 6.2, 2020, pp. 281-292.

[3] Cao, R., Meng, K., Sun, K., & Zheng, Z. “Evaluation Model of Data Consistency Mechanism in Decentralized Network Application.” In 2021 IEEE 9th International Conference on Information, Communication and Networks (ICICN), 2021, pp. 389-394.

[4] Braga, Romulo Rhemo Palitot, and Arthur Augusto Barbosa Luna. "Dark Web and Bitcoin: An Analysis of the Impact of Digital Anonymate and Cryptocurrencies in the Practice of Money Laundering Crime," Direito e Desenvolvimento, vol.50, pp.270, 2018.

[5] Berdik D, Otoum S, Schmidt N, et al. “A survey on blockchain for information systems management and security.” Information Processing & Management, vol.58, no.1, pp.102397, 2021.

[6] Xiaomeng J, Fan Z, Shenwen L, et al. “Data Analysis of Bitcoin Blockchain Network Nodes,” 2020 15th IEEE Conference on Industrial Electronics and Applications (ICIEA). IEEE, 2020, pp.1891-1895.

[7] Lee C, Maharjan S, Ko K, et al. “Toward detecting illegal transactions on bitcoin using machine-learning methods” International Conference on Blockchain and Trustworthy Systems. Springer, Singapore, 2019, pp.520-533.

[8] Gaihre A, Luo Y, Liu H. “Do bitcoin users really care about anonymity? an analysis of the bitcoin transaction graph” 2018 IEEE International Conference on Big Data (Big Data). IEEE, 2018, pp.1198-1207.

[9] Van Wegberg, Rolf, Jan-Jaap Oerlemans, and Oskar van Deventer. "Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin," Journal of Financial Crime, 2018.

[10] Hirshman, Jason, Yifei Huang, and Stephen Macke. "Unsupervised approaches to detecting anomalous behavior in the bitcoin transaction network," Technical report, Stanford University, 2013.

[11] Pham, Thai, and Steven Lee. "Anomaly detection in the bitcoin system-a network perspective," arXiv preprint arXiv:1611.03942, 2016.

[12] Pham, Thai, and Steven Lee. "Anomaly detection in bitcoin network using unsupervised learning methods." arXiv preprint arXiv:1611.03941, 2016.

[13] Monamo, Patrick, Vukosi Marivate, and Bheki Twala. "Unsupervised learning for robust Bitcoin fraud detection," 2016 Information Security for South Africa (ISSA). IEEE, 2016, pp.129-134.

[14] Monamo, Patrick M., Vukosi Marivate, and Bhesipho Twala. "A multifaceted approach to Bitcoin fraud detection: Global and local outliers," 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE, 2016, pp.188-194.

[15] Weber M, Chen J, Suzumura T, et al. Scalable graph learning for anti-money laundering: A first look[J]. arXiv preprint arXiv:1812.00076, 2018.

[16] Weber, Mark, et al. "Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics," arXiv preprint arXiv:1908.02591, 2019.

[17] Alarab, Ismail, Simant Prakoonwit, and Mohamed Ikbal Nacer. "Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain." Proceedings of the 2020 5th International Conference on Machine Learning Technologies, 2020, pp.23-27.

[18] Alarab, Ismail, and Simant Prakoonwit. "Graph-Based LSTM for Anti-money Laundering: Experimenting Temporal Graph Convolutional Network with Bitcoin Data," Neural Processing Letters, 2022, pp.1-19.

[19] Chen, Binjie, Fushan Wei, and Chunxiang Gu. "Bitcoin Theft Detection Based on Supervised Machine Learning Algorithms," Security and Communication Networks 2021, 2021.