Deep Set Classifier for Financial Forensics: An application to detect money laundering

Jonathan Pan
Home Team Science and Technology Agency
Jonathan_Pan@htx.gov.sg

Abstract— Financial forensics has an important role in the field of finance to detect and investigate the occurrence of finance related crimes like money laundering. However, as with other forms of criminal activities, the forensics analysis of such activities is a complex undertaking with attempts by the adversaries to constantly upgrade their ability to evade detection. Also, the extent of the volume and complexity of financial activities or transactions further complicates the task of performing financial forensics. Machine Learning or Artificial Intelligence algorithms could be used to deal with such complexities. However, the challenge of limitedly available labeled datasets especially with fraudulent activities limits the means to develop efficient algorithms. Additionally, the complexity of defining precise search patterns of evasive fraudulent transactions further complicates this challenge. In this paper, we developed a novel deep set classifier algorithm based on meta learning and applied it to deal with the complexity deriving patterns of interest with sample of limitedly labelled transactions to detect fraudulent cryptocurrency money laundering transactions. We a unique approach to train our model with progressive provision of samples and the test result exceeds leading research algorithms.

Keywords— Financial Forensics; Deep Set; Meta Learning and Zero Shot Learning; Cryptocurrency Money Laundering

I. INTRODUCTION

Financial forensics is a field within finance that applies criminal investigation and forensic skills with financial auditing to uncover and analyse financial criminal activities originating within or external to an organization. Financial crime is crime committed against property in its various form that including financial monetary resources or in other contemporary forms like cryptocurrencies. One such financial crime is money laundering that seeks to evade prevention, detection and prosecution of any movement of financial proceeds originating from criminal activities. According to World Economic Forum, the current regime to deal with money laundering is not adept to deal the scale of crime where illicit proceeds from criminal activities amount to 2-5% of the global GDP (or $2 trillion USD) [1].

As with other domains of forensic science, financial forensics faces the challenge of the dealing with hidden tracks from evasive tactics used by criminals. The problem becomes further compounded by the need for investigators or auditors need to spot weak signals from the huge volume of data to analyze. They would also need to ensure keeping a low measure of false positive detections, or misclassification of valid transactions, as these would put a significant strain on the limited investigative resources [2]. False negatives, or misclassification of fraudulent transaction as licit, could have disastrous outcomes. Even with the ability to detect accurately, their limited occurrences or discovery opportunities would further constrain the investigators and auditors to codify automation signature rules to uncover them. As fraudulent transactions are limitedly uncovered progressively by investigators or auditors, the core consideration with this research work is whether uncovered transactions could provide the means or patterns to uncover other similar transactions?

In this research work, we develop a deep set classification algorithm that implements a deep learning based probabilistic set theory binary relation operator that evaluates the membership of a transaction under evaluation to a provided set of transactions. We hypothesis that fraudulent transactions may contain synonymatic pattern with other fraudulent transactions and they could be identified by evaluating their memberships to a given fingerprint pattern representation derived from a set of samples. We applied this empirically to real world financial forensics datasets specifically containing Bitcoin money laundering transactions to identify illicit transactions.

We opined that our research work would contribute to academically and practically in the following manner.

- The novel algorithmic construct derives the unique representation pattern from a given set of sample transactions to predict a query transaction’s membership association using a combination of Meta based contrast learning and zero shot learning. Additionally, a unique approach is used to train such model to achieve high accuracy classification.
- Based on our best knowledge, we are the first to apply our uniquely constructed deep set classifier model to detect fraudulent cryptocurrency based money

© 2022 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other users for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
laundering. Our model’s performance exceeds other leading algorithms.

In the next section, we will cover background information of financial forensics and deep set theory. This is followed by a review of recent research work in algorithms to detect money laundering and deep set applications. We then cover the construct of our algorithm followed by the design of experiment with its evaluation criteria. This paper concludes with a conclusion and its future research direction.

II. BACKGROUND INFORMATION

In this section, we briefly explain what is money laundering, which one form of financial crime, and the use of cryptocurrency by criminal entities to clean dirty money in cyber space. We will also briefly explain the concept of Deep Set to which our algorithm was developed to operate on.

A. Money Laundering

Money Laundering involves the abuse of financial systems to clean funds that illegally acquired to become legitimate using different methods to evade detection and hide the source of the funds [3]. Typically, money laundering involves three stages [4]. The first stage is known as “placement” where funds are introduced in the financial system. The next stage is known as “layering” where the complex financial transactions are used to hide the illegal source of the funds. The final stage is known as “integration” where the financial benefits or gains are acquired from the use of these illegal funds. Measures to deal with money laundering, also known as Anti-Money Laundering (or AML), is typically applied during the placement stage. With the move towards digitalization of finance, the detection of money laundering grows in complexity due to the vast extent of opportunities for such fraudulent transactions to occur within myriad of voluminous and fast online exchanges of financial transactions. Another challenge is the need for multi-step and multi-level classification when such fraudulent transactions are uncovered that involve the need to perform inspection of multiple entities including the banks and law-enforcement and inspection of multiple levels of transactional graduality [5].

Laundering tactics have now kept up with times and moved into the cryptocurrency space. Oosthoek and Doerr wrote a paper [6] about the trends of cryptocurrency money laundering. Typically, such laundering occurs as a post breach tactic with the intent to obfuscate stolen cryptocurrency movement. Such cleansing movement of cryptocurrency funds may end with the conversion to fiat assets or government backed currencies. This forms part of the larger complex operations used by adversaries or criminal actors.

B. Deep Set

The deep set generic framework developed by Zaheer et. al [8] is designed and proposed to deal with the setting where input and possibly output instances in a deep learning task are set related. A set represents a collection of objects where these objects have defined characteristics or patterns. Membership to the collection is distinguishable and the order is irrelevant. Objects in the collection can be sets themselves such that a set of sets can be formed. In the context of neural networks based deep learning algorithms, a trained model can learn the set structure for a collection and be invariant to the order of objects in the set. The following are the properties of Deep Set.

- Property 1 A function $f: 2^X \rightarrow Y$ acting on sets must be permutation invariant to the order of objects in the set, that is, for any permutation $\pi: f([x_1,\ldots,x_M]) = f([\pi(x_1),\ldots,\pi(x_M)])$
- Property 2 A function $f(X)\mid f(X')$ operating on a set $X$ having elements from a countable universe, is a valid set function, i.e., invariant to the permutation of instances in $X$, iff it can be decomposed in the form $\phi(\Sigma_{x \in X} \phi(x)) \phi(\Sigma_{x \in X'} \phi(x))$, for suitable transformations $\phi$ and $\rho$.
- Lemma 3 The function $f_\lambda: \mathbb{R}^M \rightarrow \mathbb{R}^M$ $f_\lambda : \mathbb{R}^M \rightarrow \mathbb{R}^M$ defined above is permutation equivariant iff all the off-diagonal elements of $\Theta$ are tied together and all the diagonal elements are equal as well. That is, $\Theta=\lambda I+\gamma(11^T)\in\mathbb{R}^{M \times M}$ $\lambda,\gamma \in \mathbb{R}$ $\mathbf{1}=[1,...,1]^T \in \mathbb{R}^M$ $\mathbf{I} \in \mathbb{M}^{M \times M}$ is the identity matrix. This result can be easily extended to higher dimensions, i.e., $X = \mathbb{R}^C X = \mathbb{R}^C$ when $\lambda, \gamma$ can be matrices.

III. RELATED WORK

In this section, we review the current research machine learning (ML) and artificial intelligence (AI) solutions developed to detect money laundering. Also related research on using ML or AI for set prediction.

A. ML / AI for Money Laundering

According to Kute et. al [5], machine learning (ML) algorithms like Random Forest, K-means Clustering, Support Vector Machines and deep learning (DL) algorithms like Autoencoder and Graph Convolutional Neural Networks have been studied for money laundering detection. These algorithms performed well with classical supervised or unsupervised learning training and evaluation approaches. However, these solutions face the challenge of detecting the continuously changing forms of fraud and constrained by the availability of fraud labels.

Chen et. al [7] argued that many of ML based approaches adopt the assumption that money laundering instances are outliers that exhibits significantly different behaviours or feature indicators from the majority of the financial transaction that are legitimate. The most common ML approaches involve the use of unsupervised anomaly detection methods to model licit behaviours and to detect the instances that deviate from the norm. Such approaches have low false positive rates and good detection rates. Despite their positive
results, the authors were openly doubtful of the reproducibility of good results in real world settings with intricate patterns due to its evasive nature and in-complete labels caused by the rarity of illicit transactions relative to the high volume of licit ones. Other recent research algorithmic development work in detecting money laundering have produced good accuracy predictions [13][15][17]. Our research work seeks to do better.

B. Set Classification

Set classification is about training a model to predict the membership of an unordered object to a collection with unknown interrelations. From our survey, we noted that there are few yet recent research work in developing models for set classification. One such is by Zhang et al [9] who proposed a general model for predicting sets that respects the structure of sets. Their model takes a single feature vector as input to predict bounding boxes of the set of objects and attributes of these objects in an image. In another work [10], a general model was developed that uses a stochastically augmented prediction algorithm to perform multiple set predictions and reflecting the possible variations in the target set to perform density estimation, predict the set of object locations, detect subset anomalies from facial images. However, there was no noted work that applied set prediction or classification to detect financial fraudulent transactions.

IV. MODEL

Our model construct is based on meta-learning that learns contrastive comparison to evaluate the membership of a query point against a given set of positive and negative samples. The model is then further trained using a form of zero shot learning training approach where the model iteratively identifies candidate datapoints to populate its knowledge repositories of samples that qualify and disqualify set membership with the intent to further hone the accuracy of the model.

A. Contrastive Meta Learning

Our algorithmic design is primarily based on meta learning. This is a subdomain of machine learning algorithms designed to perform automatic learning. It is ideally suited for solving learning problems. Unlike popular Supervised learning or Unsupervised learning algorithms that are not optimal for this task of learning from limited data results, Meta Learning algorithms focus on learning to learn that would result in acquiring knowledge versatility to learn new skills or adapt to new environment with minimal training examples [11]. For our meta-learning algorithm, we used the basic model based Prototypical network [11] that converts the embedding from the encoder from curated samples that represents the support set to its corresponding pattern prototype. Our algorithm takes as inputs a support set of samples that represents the positive samples and uses a fixed support set that represents the negative samples. The algorithm computes the prototypes for these two support sets. The computed positive prototype is represented by the prototypical representation derived from the provided set of positive samples. The negative prototype is derived from the origin of the feature embedding space which is constant as the origin would not change within the same of problem domain. The prototypical computation is done with prototype representation \( \mathbf{C}_k \mathbf{C}_k \) or centroid of the support sample set \( S_k \), and \( k \) either represents the positive or negative samples. The centroid is computed using \( f_k \mathbf{f}_k \) with \( \mathbf{Q} \mathbf{Q} \) as learnable parameters.

\[
c_k = \frac{1}{|S_k|} \sum_{x_i \in S_k} f_k(x_i)
\]

With the derived pattern prototypes, we apply contrastive learning to learn the objective function of measure pattern similarity through positive and negative examples. An instance of positive example is a set of datapoints as samples and a query datapoint the training dataset with the same class label. The negative example would use a different class label. However, to address the constraint of having limited labeled data or imbalanced class labels, the algorithm needs to learn how to recognize matching patterns from the same class label and recognize those that do not. This non-linear similarity measurement uses the Euclidean distance of the positive and negative prototypes against the query datapoint.

\[
p_k(y = k|x) = \text{softmax}(-d(f_k(x), c_k))
\]

\[
\mathcal{L}(\phi) = -\log p_y = k|x'
\]

We optimized our model’s objective function with the following loss function expression when the model is given samples to represent the set representations \( \mathbf{Q} \mathbf{Q} \) (which is the positive samples), the origin \( \mathbf{O} \mathbf{O} \) (which is the negative samples) and query datapoint \( \mathbf{Q} \mathbf{Q} \).

\[
\delta(x^t, x^q) = \begin{cases} \max \|p_y = t|x \|, t=q & \text{max} \|p_y = n|x \|, t\neq q \end{cases}
\]

B. Zero Shot Learning

The Zero Shot Learning (ZSL) characteristic of our algorithm that performs class to class similarity comparison. Typically during inference, unknown query point which is represented as a financial transaction is given to our model to analyze. The embeddings of the query point are compared against the set samples’ embeddings. Formally, the ZSL algorithmic module has the function \( \mathbf{f} \mathbf{f} \) that maps \( \mathbf{X} \rightarrow \mathbf{Y} \) \( \mathbf{X} \rightarrow \mathbf{Y} \) where \( \mathbf{f} \mathbf{f} \) is the Zero Shot learning module [12].

\[
f(x, W) = \max_{\mathbf{W}} F(x, y; W)
\]
Typically, Zero Shot Learning is applied in test time with the aim to assign a test image to an unseen class label. However, with our work, we applied ZSL to further train our model, in a supervised manner, to gather more samples that belong and do not belong to the set. The gathered list of samples is based on incorrect classifications. This list is further grouped into two sub-lists. The first is $Y_p$ which carries the list of incorrect classifications of type I error or False Positives. The other is $Y_n$ with the list of type II errors or False Negatives. As the base contrastive meta-learning model is formulated to take as inputs a defined size of samples, hence the model would need to select datapoints that has the highest misclassification based on the inference probabilistic value for ZSL training iteration. We chose this selection criteria to correct the model’s deepest invalid biases. The ZSL training iterates each training cycle with the model progressively enlarging the support sets of elements or transaction samples $D_t$ that represents the group of elements to be used to evaluate the membership of an element under query against the set.

Zero-Shot Learning Training Stage

1: Require: $D_t$  \hspace{1cm} \triangleright \text{initial list of fraudulent transactions}
2: Require: $D_q$  \hspace{1cm} \triangleright \text{list of labeled transactions}
3: $P \leftarrow \text{trained meta-based contrast learning model}$
4: While Not End of Learning do
5: \hspace{1cm} $Y_p, Y_n := \text{Null}$
6: \hspace{1cm} for $x \in D_q$ do
7: \hspace{2cm} if $P(x, D_t) \not\in \text{Label}(x)$ then
8: \hspace{3cm} if $\text{Label}(x) = \text{Fraud}$ then
9: \hspace{4cm} $Y_p := Y_p \cup x$
10: \hspace{1cm} else
11: \hspace{2cm} $Y_n := Y_n \cup x$
12: \hspace{1cm} $D_t := D_t \cup \text{set}(\text{argmax}(Y_p), \text{Fraud})$
13: \hspace{1cm} $D_t := D_t \cup \text{set}(\text{argmax}(Y_n), \text{Non-Fraud})$
14: end

Figure 1. Pseudocode for Zero Shot Learning Training

The ‘End of Learning’ is defined as the condition to end the ZSL training. This could be when the ZSL training saturates in finding any new element that the model misclassifies. After the ZSL training, the collection of acquired sets of samples will then be used to classify the test query points from the apportioned test dataset.

V. METHODOLOGY AND ANALYSIS

In our design of experiment setup, we chose representative datasets that is commonly used by other research work to evaluate our model.

A. Datasets

We used a real-world derived dataset of money laundering occurrences with the Bitcoin cryptocurrency. The dataset was released by Elliptic which is a company dedicated to detecting financial crime in cryptocurrencies [14]. This dataset consists of Bitcoin transactions with an estimated value of USD 6 billion. The datasets compromises of 203,769 transactions with 234,355 Bitcoin payment flows. 21% of the transactions is labeled as licit that includes transactions originating from exchanges, wallet providers, miners and other forms of licit online services. About 2% of the transactions are labelled illicit and the rest are labelled as unknown. For our research, we would group the licit and unknown as one class. The illicit transactions could originate from scams, malware, terrorist organization and Ponzi schemes. The rest of the transactions are unlabeled. Past research work typically represents such transactions graphically with each Bitcoin transaction being a transfer from one Bitcoin address to another that is represented as nodes in the graph. The edges in the graph represent the flow of Bitcoins between transactions. Each transaction within the dataset has 166 features. 94 of the 166 represent information about the transaction like timestamps and number of inputs and outputs related to that transaction and its transaction fees. The rest of the features are statistically compiled from information about the transaction such as the minimum, maximum, and standard deviation. All features, except for the time-step which we removed in our research work, are fully anonymized and normalized.

The following table summarizes the two distinct sets (fraudulent and non-fraudulent) for each dataset. The model will subsequently be trained to perform set prediction based on these two datasets with imbalanced classes.

| Characteristics | Elliptic Dataset |
|-----------------|------------------|
| No. of nodes    | 203,769          |
| No. of edges    | 234,355          |
| No. of features | 166              |
| No. of class labels | 3            |
| No. of illicit transactions | 4,545        |
| No. of Licit transactions  | 42,019        |
| No. of Unknown transactions | 187,791    |

Table 1. Characteristics of Elliptic Dataset containing real-world Bitcoin Money Laundering Transactions

B. Evaluation Metrics

We adopted the evaluation metrics used by other research work so that we could perform performance comparisons. Hence, we used precision and recall to assess the accuracy of the model to detect fraudulent transactions for both datasets. Finally, we used $F1$ score to measure the harmonic mean of precision and recall.

$$\text{Precision} = \frac{TP}{TP + FP} \quad \text{Precision} = \frac{TP}{TP + FP} \quad \text{6}$$

$$\text{Recall} = \frac{TP}{TP + FR} \quad \text{Recall} = \frac{TP}{TP + FR} \quad \text{7}$$
\[ F1 score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \]

TP (True Positive) represents the number of correctly classified fraudulent transactions and FP (False Positive) is the number incorrect non-fraudulent classifications. FN (False Negative) is the number of incorrect classifications of fraudulent transactions.

C. Model Preparation and Evaluation

As described earlier, our model construct that consists of contrastive meta learning and zero shot learning required a different form of model training. Hence, we divided the dataset in three divisions. One set or 40% of the entire dataset is to train the contrastive meta learning model with positive and negative training sample provided. For our experiment, we configured the support set to contain ten elements. This is an arbitrary value which will be studied further in future work. In this stage of training, the model would adjust its weights to maximize its accuracy to recognize matched or unmatched queries against the provided sample sets. To further stretch the classification challenge with our model, we used only licit and unknown transactions for contrast training whether a set of liked labeled samples matches with the transaction being compared. The intent is to train the model to recognize like and unlike patterns.

The next stage of training focused on the zero-shot learning. The objective of this stage of training was to derive the support set of elements that would represent the fraudulent and non-fraudulent transactions. This involved gathering those sets of sample sets to classify the transactions and improve the accuracy prediction of the model. The approach used is a supervised learning approach where the labels of the designated training dataset is to identify false positives and negatives that would in turn create a list of sample sets to tune the model predictions. This training dataset amounts to 40% of the entire dataset containing licit, illicit and unknown transactions. We grouped the licit and unknown transactions under one class as non-fraudulent transactions and left illicit transactions as the only form of fraudulent transaction. For the Bitcoin money laundering dataset, we manually chose one set of illicit transactions as the True Positive sample set. We then iteratively run the model to identify False Positives and False Negatives. With this dataset, we considered licit and unknown transactions as one class while grouping the illicit ones as the other class to detect.

Finally, the model with the list of support sets of samples evaluated the test datasets that represents 20% of the entire dataset. The test dataset contained licit, unknown and illicit transactions. The accuracy measurement was then compared against the prevailing leading research using this dataset of cryptocurrency money laundering.

D. Results and Analysis

As our model construct involved two stages of learning with the second stage with zero-shot learning used to gather a list of elements that would best represent the sets for fraudulent transactions, hence we first analyzed this stage of learning progress of the model using precision, recall and F1 scores. The following chart shows the progressive improvements made as the model gathers more elements into its support set for the qualifiers for fraudulent transactions and support set for non-fraudulent transactions for money laundering dataset.

![Image](chart.png)

Figure 2. Zero-Shot Learning Training Accuracy Measurements

Our model progressively improved its classification accuracy with each iteration of support elements gathering that was subsequently included into the support sets for each transaction type (fraudulent or not).

The models were subsequently tested with the designated test datasets. We compared our results against other leading research work.

| Models | Precision | Recall | F1 score |
|--------|-----------|--------|----------|
| SNN [13] | 0.894 | 0.899 | 0.897 |
| O-DT [13] | 0.935 | 0.934 | 0.935 |
| RandomForest AF + GNE [15] | 0.958 | 0.715 | 0.815 |
| XGB AF + GNE [15] | 0.986 | 0.692 | 0.813 |
| GCN [16] | 0.899 | 0.678 | 0.773 |
| Skip-GCN [17] | 0.812 | 0.623 | 0.705 |
| EvolveGCN [17] | 0.850 | 0.624 | 0.720 |
| Inspection-L AF + GNE (RF)[18] | 0.972 | 0.721 | 0.828 |
| Ours | **1.000** | **0.967** | **0.983** |

Table 2. Performance Comparison

Comparatively, our model performed better than other leading algorithms in detecting fraudulent bitcoin transactions with higher Precision, Recall and F1 scores. The following table details the total number of support elements needed for each set class for each dataset.
Table 3. Support Elements After Zero-Shot Learning Training

| Transaction Type   | Record Count (%) | Support Elements after ZSL Training (%) |
|--------------------|------------------|----------------------------------------|
| Fraudulent (Illicit) | 4,545 (2.3%)     | 40 (0.88%)                              |
| Non-Fraudulent     | 199,224 (97.7%)  | 30 (0.02%)                              |

From this experiment, our model only requires a small number of support elements to detect fraudulent transactions. It requires far fewer number of support elements for non-fraudulent transactions. This could be so as there may be more pattern variations with fraudulent transactions.

VI. CONCLUSION AND FUTURE DIRECTIONS

In this research, we develop algorithmic construct that uniquely combines contrastive meta learning and zero shot learning to perform deep set classification of set membership of a query to a set defined by a set of samples. We trained the model through a two-stage training approach where the model is first trained to learn to perform contrast comparison with positive and negative examples. This is then followed by a zero-shot learning training iteration to draw out a list of samples as support elements to sharpen the accuracy of model before its evaluation. The trained model performed better than current leading models on the cryptocurrency money laundering dataset.

The next step is to conduct further research into the model hyper-parameters namely with the size of the sample set, an optimized training formulation for the zero-shot learning stage and the optimization of data embedding space for contrastive comparison. Finally, to explore algorithmic constructs that would further implement the other concepts of set theory beyond membership.

REFERENCES

[1] World Economic Forum, “Global Coalition to Fight Financial Crime”. Accessed: Jul. 7, 2022. [Online]. Available: https://www.weforum.org/projects/coalition-to-fight-financial-crime.

[2] Wronka, C., “Cyber-laundering: the change of money laundering in the digital age”, Journal of Money Laundering Control, Vol. 25 No. 2, pp. 330-344. https://doi.org/10.1108/JMLC-04-2021-0035, (2022).

[3] Study Guide for The CAMS (Certified Anti-Money Laundering Specialists). [Online]. Available: https://www.acams.org, 2012.

[4] F. A. T. Force, “What is Money Laundering”, Accessed: Feb. 26, 2021. [Online]. Available: https://www.fat-gafi.org/faq/moneylaundering, 2021.

[5] Kute, D.V., Pradhan, B., Shukla, N. and Alamri, A., “Deep learning and explainable artificial intelligence techniques applied for detecting money laundering—a critical review”, IEEE Access, 9, pp.82300-82317, 2021.

[6] Oosthoek, K and Doerr, C, “Cyber Security Threats to Bitcoin Exchanges: Adversary Exploitation and Laundering Techniques”, IEEE Transactions on Network and Service Management 18, 2 (2020), 1616–1628.

[7] Zhiyuan Chen, Le Dinh Van Khoa, Ee Na Teoh, Amrill Nazir, Ettikan Kandasamy Karuppiiah, and Kim Sim Lam. 2018. Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. Knowledge and Information Systems 57, 2 (2018), 245–285.

[8] Zaheer, M., Kottur, S., Ravanbakhsh, S., Poczos, B., Salakhutdinov, R.R. and Smola, A.J., “Deep sets”, Advances in neural information processing systems, 30, 2017.

[9] Zhang, Y., Hare, J. and Prugel-Bennett, A., “Deep set prediction networks”, Advances in Neural Information Processing Systems, 32, 2019.

[10] Zhang, D.W., Burghouts, G.J. and Snoek, C.G., “Set prediction without imposing structure as conditional density estimation”, arXiv preprint arXiv:2010.04109, 2020.

[11] J. Smell, K. Swersky, and R. S. Zemel, “Prototypical networks for few-shot learning”, Neural Information Processing Systems, 2017.

[12] Y. Xian, C. H. Lampert, B. Schiele, and Z. Akata. Zero-shot learning—a comprehensive evaluation of the good, the bad and the ugly. arXiv preprint arXiv:1707.00600, 2017.

[13] A. A. Badawi and Q. A. Al-Haija, "Detection of money laundering in bitcoin transactions," 4th Smart Cities Symposium (SCS 2021), 2021, pp. 458-464, doi: 10.1049/icp.2022.0387.

[14] Mark Weber, Giacomo Domeniconi, Jie Chen, Daniel Karl Weidele, Claudio Bellei, Tom Robinson, and Charles E. Leiserson. 2019. Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics. arXiv preprint arXiv:1908.02591 (2019).

[15] D. Vassallo, V. Vella, J. Ellul, Application of gradient boosting algo- rithms for anti-money laundering in cryptocurrencies, SN Computer Science 2 (3) (2021) 1–15.

[16] I. Alarah, S. Prakoonwit, M. I. Nacer, Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain, in: Proceedings of the 2020 5th International Conference on Machine Learning Technologies, 2020, pp. 23–27.

[17] M. Weber, G. Domeniconi, J. Chen, D. K. I. Weidele, C. Bellei, T. Robinson, C. E. Leiserson, “Anti-money laundering in bitcoin: Experiment- ing with graph convolutional networks for financial forensics”, ACM SIGKDD International Workshop on Knowledge discovery and data min- ing, 2019.

[18] W. W. Lo, S. Layeghy and M. Portmann, Inspection-L: Practical GNN-Based Money Laundering Detection System for Bitcoin. arXiv preprint arXiv:2203.10465, 2022.