SOLENT UNIVERSITY, SOUTHAMPTON
FACULTY OF BUSINESS, LAW, AND DIGITAL TECHNOLOGIES

MSc Applied Artificial Intelligence and Data Science
Academic Year 2021-2022

ANOMALY DETECTION IN BITCOIN TRANSACTIONS USING CLASSIFICATION MODELS

Supervisor: Dr. Peyman Heydarian
September 2022

This report is submitted in partial fulfilment of the requirement of Solent University for the degree of MSc Applied Artificial Intelligence and Data Science

Acknowledgments

Without the help of the Almighty God, who oversaw this project, it would not have been feasible to complete this project. I can't begin to convey how grateful I am to Peyman Heydarian, my supervisor, for his feedback and invaluable patience. I would not have been able to embark on this journey without his freely shared knowledge and insight.

Additionally, I appreciate my classmates and cohort members. especially Odesola Peter, Babalola Idris, Olabisi Dabi, and Ruth Babatunde for their moral support and late-night feedback sessions. I also extend my gratitude to the university's librarians who had an impact on and inspired me.

Dedication

It is with genuine gratitude and warm regard that I dedicate this work to my family because of their confidence in me, I have maintained a positive attitude and strong drive throughout this journey.

ABSTRACT

Long-term research has been conducted into the issue of anomaly detection in bitcoin transactions, and a lot of different approaches based on network analysis have been put up as potential solutions. Although there are several outcomes that look to have quite a bit of potential, none of the methods appear to be definitively better than the others. The Elliptic dataset was used in this study and various machine learning algorithms were tested and graph analyses on Bitcoin transactions in order to classify Bitcoin transactions as either licit or illicit. To deal with the evident class imbalance in the illicit class on the dataset. the model is trained using Autoencoder. After that, several machine learning classifiers were put through their paces, and four of them emerged victorious. Random Forest, Logistic Regression, XGBoost, and Multi Layered Perception were shown to have the greatest overall performance when compared to the other classifiers. These are the top four classifiers.

Table of Contents

CHAPTER ONE

INTRODUCTION

1.1 Background Study

Before being made available as open-source software in 2009, the concept of Bitcoin was first put out by Satoshi Nakamoto who is an unidentified individual (or group of people). A peer-to-peer cryptocurrency; Bitcoin operates as a decentralized, global system for transferring digital currency between users. Bitcoin transactions are processed and authenticated by network nodes before being recorded in the blockchain, a public ledger. Blockchain is the foundation for all Bitcoin transactions. It offers a ground-breaking decentralized consensus method for securely preserving money transfers, transactions and other data records without involving third-party authorities. Every transaction in the bitcoin blockchain is broadcast to all peers present in the network and verified by a collection of nodes known as miners to ensure its integrity, validity, and authenticity.

Bitcoin is distinct from traditional online banking in form of its continuous operation on a peer-to-peer network (P2P) rather than being associated with any centralized third parties, such as internet banking, notaries, or other traditional online financial institutions that perform and authorize electronic payments. Instead, by having total control over how and when to spend digital currency, Bitcoin users possess complete control over what they choose to do with their own money. With more people becoming aware of Bitcoin, more customers are being drawn to utilize this payment method in a variety of businesses. People typically praise Bitcoin for being quick, easy, tax-free, and innovative. Nothing is ever perfect, though. Since they offer new dangers owing to their lack of

centralized control and law enforcement, confidentiality, reliability, and security of Bitcoin have been under scrutiny. Furthermore, to guarantee the dependability and trustworthiness of a decentralized system of money transactions, every Bitcoin owner and operator should have a secure location to handle money and safeguard their own property. (Rahouti, Xiong and Ghani 2018). This cryptocurrency is currently worth about $441,349,756,150.96 and is regularly traded all over the world.

In 2022, fraudsters have indeed stolen roughly $2 billion in cryptocurrency – even though the year is just halfway through. An article by Cheyenne DeVon (2022) relays leader and co-founder of crypto payment platform CoinsPaid Max Krupyshev speech that says, “Despite the misconception that cryptocurrency is anonymous, it remains easier to run away with coins or tokens, I don’t think that crypto hackers are stronger than the ‘usual’ kinds, it’s just that crypto platforms are new and hold valuable assets.”. Though DeFi has faced much of the brunt of the attacks, Protocols of Decentralized finance (DeFi), which are inherently susceptible to hacks, are increasingly being targeted by malicious users. DeFi projects are often implemented on the Ethereum blockchain, and users may earn interest, borrow money, as well as utilize their NFTs as leverage. However, this study is primarily based on Bitcoin blockchain.

1.1 Problem Statement

It has already been shown that the Bitcoin ecosystem, as well as its network structure, is susceptible to a broad variety of illegal activities and assaults. There have been several investigations into the Bitcoin system, including market return, anomaly detection, and predicting volatility. Several research have also concentrated on the application of Machine Learning techniques to the problem of anomaly detection in Bitcoin networks, such as the identification of fraudulent activity and unusual activities or transactions. However, there have only been a handful of research conducted on the Bitcoin blockchain. Examining the Bitcoin

network from the perspective of a complex network is essential because doing so may assist in explaining some of the mysteries that surround contemporary blockchain systems.

1.2 Justification

However, there is still very little study being done on the Bitcoin transaction network. Existing research on the Bitcoin network is mostly concerned with long-term, comprehensive data analysis of Bitcoin's overall infrastructure (Lischke and Fabian 2016), (Nerurkar *et al*. 2021), or the identification of transaction patterns (Wu *et al*. 2022), but it lacks both a thorough analysis of network characteristics and computationally effective algorithms for networks analysis. Along these lines, in this study, an intensive focus on Machine Learning techniques and methods in the detection of malicious and unusual activities in the Bitcoin transaction is conducted with the aid of Autoencoders.

1.3 Research Aim & Objectives

The purpose of this study is to identify anomalies in Bitcoin transactions by describing the distance between a given transaction and a known illicit transaction in the Bitcoin network. This will be done with the help of graph convolutional networks and Autoencoders.

Objectives:

1. Develop a predictive model that classifies licit transactions and an illicit transaction
2. What kind of effects do the features of the Bitcoin network that are designed to identify illegal transactions have?
3. Develop a Graphical User Interface GUI, that can be put forth as a machine learning model.

1.4 Scope

The scope of the study is primarily focused on the binary classification task using a variety of auto-encoders to identify illegal node transactions and transaction screening to assess the risk involved with a given transaction between bitcoin wallets. The purpose of the study is to determine whether or not illicit node transactions can be screened out.

CHAPTER TWO

LITERATURE REVIEW

2.1 Related Works

Few research studies have examined ways to identify anomalies throughout the Bitcoin blockchain during the past few years, in this section a brief summary of studies in the area of anomaly detection in financial institutions are arranged in a chronological order. (Zambre and Shah 2013) research attempted to uncover the distinctive characteristics of users that commit various kinds of heists, as well as to find the characteristics that distinguish rogue users from good ones using feature selection while to group users together; K-Means Clustering is used. It was noticed that applying K-Means on all features yielded subpar results when attempting to cluster users based on the features, as did scaling and normalizing of features. The developed k-Means model was unable to classify the fraudulent users' nodes in a distinct cluster from the good users' cluster. Following testing of several feature combinations, a selective feature combination was identified. This model was capable of distinguishing between legitimate and fraudulent users. The theory was that the other nodes in the fraudulent user's cluster would represent the Bitcoin Network's significant mixing services; however, they have no recorded data on mixing services. However, this approach is unlikely to be particularly effective for fraudulent activities that occur in little increments over a lengthy period of time.

The goal of the study by (Hirshman, Huang and Macke) used machine learning methods to analyse a dataset of bitcoin transactions, as well as to investigate the bitcoin network's anonymity guarantees. The study then describes an initial attempt to explore the dataset by clustering hubs (the used term for users with a large number of transactions) based on a specific feature set, initially using the K-means algorithm followed by an unsupervised learning algorithm, "RolX," which designates the users to different roles. The article mentions some interesting,

anomalous behaviour that was identified because of the unsupervised dataset rearrangement. A significant bitcoin transaction network was found to have anomalies using unsupervised learning methods. the study was able to identify certain users who executed transactions in an unusual manner, implying money laundering. Unfortunately, there was no method of validating such allegations since there was a lack of labelled data pointing to examples of these alleged mixing services. However, the study emphasises that it might open the way for future clustering algorithms, particularly by enabling users to choose variables that are more revealing of data patterns. The unsupervised learning algorithms used, Kmeans and RolX, were successful in finding unusual behavior in the network.

(Monamo, Marivate and Twala Aug 2016) examined the application of trimmed k-means, which is competent for simultaneous object clustering and fraud detection in a multivariate setting, to identify fraudulent Bitcoin transactions. The primary purpose of the research is to identify and classify Bitcoin network anomalies based on transaction patterns, and to evaluate the efficacy of anomaly detection algorithms utilizing public Bitcoin transaction data from the blockchain. (Zambre and Shah 2013) developed synthetic node data that mirrored the patterns of the three analysed heists. It was proposed that K-means clustering can group instances together and that LOF is popular for outlier identification, however, K-means clustering lacks the capacity to identify outliers and LOF does not scale well in big datasets with respect to computing time. A strategy to compensate for these limitations was suggested. It was noted that based on the suggested features collected, the algorithm is utilized to further support data supplied by prior research by (Zambre and Shah 2013) on the probable number of clusters inside the network. The second technique used, Trimmed k-means, was applied to the data set; k-means's spurious clusters were filtered out, resulting in better group structures. In terms of the number of

correctly identified anomalies, (Monamo, Marivate and Twala Aug 2016) claims that the results indicate an improvement above comparable studies' conclusion.

The study by (Haohua Sun Yin and Vatrapu Dec 2017a) used thirteen classifiers based on supervised learning, from which four demonstrated relatively high cross-validation accuracy. The Bagging and Gradient Boosting classifiers were chosen among the top four classifiers on the basis of their weighted average and per-class precision for cybercrime-related domains. It was emphasised that the dataset used in the study had a few restrictions: First, certain classes are greatly oversampled while others are significantly under-sampled, which may explain the poor performance of the models when predicting mixing. Second, the variety of classes is restricted to the categories that the data source has effectively discovered using their own clustering algorithm, thus there is no assurance that these are the only categories in the Bitcoin ecosystem.

(Pham 2018) research approaches are applicable to any environment with an intrinsic graph structure, including but not limited to computer networks, telecommunications networks, auction networks, security networks, social networks, Web networks, and financial networks. The purpose of the research was to identify the most suspect users and transactions; in this context, anomalous activity is a proxy for suspicious conduct. The use of power degree laws & densification and the Local Outlier Factor (LOF) method (followed by the k-means clustering method) on two graphs formed by the Bitcoin transaction network: one graph has users as nodes while the other graph has transactions as nodes. The power law degree distribution was applied to features other than in-degree and out-degree; if structures caused by user activity that vary considerably from these laws are identified, It may be established that an anomaly exists in the network. The lack of a broadly accepted method for evaluating algorithms for issues involving unlabelled data was identified as one of the most significant obstacles by the research.

The research conducted by (Weber 2016) presented an opportunity to find common ground between the causes of safety and financial inclusion. Elliptic Data Collection, which was provided, is the biggest labelled transaction data set that is publicly accessible in any cryptocurrency. A graph is generated and labelled from raw Bitcoin data, with nodes representing transactions and edges representing the movement of Bitcoin currency (BTC) from one transaction to the next. A transaction is considered licit (against illicit) if the entity executing the transaction (i.e., the entity possessing the private keys associated with the transaction's input addresses) falls into one of two categories. Crucially, all features are built using only publicly accessible data. Transaction screening will be done on this data to determine the risk associated with a specific transaction to and from bitcoin wallets. Each unlabelled Bitcoin transaction are classed as either illicit or licit. Logistic Regression and Random Forest are two benchmark approaches for reducing false positive rates while raising false negative rates, i.e. include more licit users while excluding more illicit users. The research found that it is difficult to expand the solely feature-based method beyond the local neighbourhood, which supports the adoption of Graph Convolutional Networks. One of the issues posed was if it was feasible to combine a Random Forest with a graph neural network, and it was recommended that before running Random Forest, the node features be augmented with the embeddings generated using GCN. According to prior studies, this approach only works somewhat. Transactions are then visualized as nodes in a graph, with edges indicating the movement of BTC from one transaction to the next. The Chronograph allows for easy research scenarios such as visually inspecting clusters and their presence over time, observing notable transfer patterns, and detecting other aberrations such as single outliers.

(Lihao Nan and Dacheng Tao Jun 2018) study was driven by the effectiveness of graph embedding in social network analysis, proposed a feature-based method for identifying mixing services, which was tested on the actual Bitcoin ledger.

The study's primary goal was to identify Bitcoin mixing services and show that Bitcoin transaction graphs have community characteristics and that a mixing service may be considered a cluster outlier. The use of various metrics and comparisons to establish the community property of Bitcoin transaction graphs was one of the primary contributions. Furthermore, the use of a novel feature extraction approach known as Bitcoin Graph Intermediate Point Detection (BGID), was believed to be more successful than traditional methods for clustering Bitcoin transaction user accounts. Finally, the method was examined on genuine Bitcoin transaction ledgers using four well-known mixing providers. The approach was shown to have three major flaws. The use of local outlier probability to assess the outlier node, which is too slow for large databases; the absence of real data labels implies that the mixing service transactions cannot be adequately described and analyzed further. Lastly, the algorithm is too slow for the size of actual Bitcoin transaction graphs, running at $O(n^2)$. Solutions to these problems were suggested.

(Cuneyt Gurcan Akcora *et al*. 2019) aimed to discover Bitcoin addresses used to store and exchange Bitcoins obtained from ransomware operations. To accomplish this aim, they offered a scalable data-driven Bitcoin transaction analytics framework that is far more effective than previous heuristic-based techniques in discovering ransomware payment-related addresses. The primary motivation for the suggested technique is the inherent capacity to monitor the entire blockchain graph and, as a consequence, follow and study the dynamics of the related blockchain topological and geometrical features at several resolutions. A novel data analytics-based methodology for detecting and predicting Bitcoin-based ransomware transactions was presented using a topological data analysis technique and unique blockchain graph-related characteristics, they achieved much greater accuracy and recall than previous heuristic-based approaches.

The study conducted by (Yining Hu *et al*. 2019) investigates the landscape of possible instances of money laundering that take place via the Bitcoin network by generating transaction graphs and providing in-depth research on numerous graph properties, money laundering activities may be distinguished from routine transactions. Among the findings is that, while some manually collected statistical and network indicators have different distributions for laundering and legitimate transactions, they are not good enough in identifying laundering activities. The model describes the graph features of money laundering transactions and highlights the distinctions between them and routine transactions. The study demonstrates that laundering transactions can be distinguished from regular transactions based on statistical and network characteristics such as the in-degree/outdegree ratio, the sum/mean/standard deviation of output values, and the number of weakly connected components—the size of the subgraph to which a transaction belongs. Despite this, the binary classification of routine transactions vs those involving money laundering cannot be reliably accomplished using these criteria. The research proposes a node2vec-based classifier that delivers the highest performance in classifying routine transactions as opposed to those involving money laundering. The study further demonstrates the robustness of the classifier by applying it to randomly chosen weeks over the course of a broad timeline of two and a half years and demonstrating that the results remain consistent during this period.

The study by (D'oro *et al*.) presented Group Anomaly Detection via Graph Autoencoders, or GADGA for short. GADGA takes advantage of recent developments in the field of graph representation learning in order to identify anomalous groups of points by focusing on the graph representation of those groups instead of their raw set representation. A set-based and graph-based baseline were compared to the results of an experimental analysis of some properties of graph autoencoders, which informed the design decisions behind the method that was used. This was followed by an empirical evaluation, which

showed that the method had superior performance. (GADGA), a method for group anomaly analysis approach that is based on graph representation learning. The reconstruction error of a graph autoencoder that has been trained on unlabeled data is used in this method to award anomaly scores to groups that are represented in the form of graphs. In order to design GADGA, the study made use of the observations on the scientific constraints of structure only graph autoencoders that were obtained by conducting experiments on toy data. Additionally, the study made sure to carefully adapt the architectures of the graph neural networks that performed the best.

The study by (Bynagari 2020) intends to investigate the use of a slope boosting computation in differentiating tax evasion activities. To explore the effectiveness of a gradient boosting algorithm in detecting money laundering. For transactional level detection, elliptic data was used in this investigation. Two structures were used to achieve the purpose of this study. The preferred structures include a module work out/test division assessment for disconnected learning as well as a preliminary inquiry for online learning. Disconnected models are generated truly as they are carried out on a definitive guide partition to work out and test gatherings in the workout/test partition investigations. However, the preliminary examination resolved to dissect online individuals by duplicating an infinite information stream, and it prepares similarly. Since of the nature of the classifiers, the evaluation required hundreds of iterations because it was non-deterministic. The Light Gradient Boosting Algorithm (LGBA) and XGBoost outperformed the Random Forest algorithm in detecting illicit transactions at both the exchange and account levels.

(Bartoletti *et al.* 2021) conducted a thorough evaluation of the scientific literature on cryptocurrency frauds, which they systematise using a unique taxonomy. A unified dataset of hundreds of bitcoin scams was created by gathering and homogenising data from various public sources. The research used this data to develop a program that automatically detects and classifies frauds

according to our taxonomy. The tool's efficacy was evaluated using common performance criteria. and then analyse the categorization findings, offering vital insights into the prevalence of scam types and the relationships between them. The study proposed a series of rules that authorities may adopt to better safeguard users against cryptocurrency frauds. the study broadly identified two sorts of frauds based on how they are indexed by websites: Bitcoin addresses given by prospective victims are examples of address-reported frauds. URL-reported scams are fake websites that was found on Web Archive. An open-source tool for classifying frauds based on our taxonomy was developed. The tool was analyzed using industry-standard procedures and metrics. The tool was utilized to perform a multilabel classification of the gathered scams, enabling to examine the prevalence and correlation of scam types, as well as the difference between pure and hybrid frauds. Although majority of the scams in our dataset are connected to Bitcoin, virtually all of them do not depend on the features of that particular blockchain, but instead, exploit the blockchain's native cryptocurrency as a method of payment. As a result, it is feasible that frauds operating on blockchains other than Bitcoin may develop in the future.

The aim of the survey by (Nicholls, Kuppa and Le-Khac 2021) was to close the gap by examining the financial cybercrime ecosystem along four axes: various fraud tactics employed by criminals; related systems, algorithms, downsides, limits, and metrics utilised to fight each fraud type. Examining the cutting-edge algorithms, models, and approaches used to combat the many aspects of financial cybercrime, it's indeed clear that it was not a simple process. The method in which behaviour is obfuscated, manipulated, and disguised makes it difficult for researchers and industry to identify, prevent, and detect malevolent criminal behaviour. The models described in this study emphasize the need of using detection approaches based on Graph/Group based Anomaly Detection in the fight against financial crime. The researchers recognise the problem of acquiring labelled datasets and the skill necessary to identify ground truths when one is

not already accessible. The researchers suggested that the respective Revenue Commissioners and law enforcement authorities of the various countries worldwide will conduct a closer examination of cryptocurrency and its integration into the public domain, resulting in increased research output, particularly in the Group/Graph based Anomaly Detection domain.

(Rao *et al*. 2021) suggested an explainable fraud transaction prediction framework, which consists primarily of a detector and an explainer. The xFraud detector can predict the validity of incoming transactions accurately and efficiently. It employs a hybrid graph neural network to learn descriptive representations from the transaction logs' informative heterogeneously typed elements. The xFraud explainer could provide relevant and human-readable explanations from graphs to help enhance procedures in the business unit. xFraud outperforms other baseline models on many assessment measures in research trials on actual transaction networks with up to 1.1 billion nodes and 3.7 billion edges, while being scalable in distributed settings. Furthermore, the study demonstrates that the xFraud explainer can offer logical explanations that greatly aid business analysis via both quantitative and qualitative assessments. xFraud is made up of a detector and an explainer. To handle transaction fraud detection in the detector; xFraud is built on a heterogeneous GNN to tackle transaction fraud detection. From a graph viewpoint, specifically classification task. Unlike traditional classification tasks, claiming that a transaction is fraudulent should be done with extreme caution to prevent negatively impacting user experience and undermining the platform's credibility. As a result, the research incorporates within the framework an explainer that may give straightforward explanations for model predictions. With these explanations, our auditors, regulators, or decision makers may understand why a transaction is identified by the detector and make better informed judgments.

The study by (Liu *et al*. 2022) aimed to solve the user complexity and variety of smart contract-enabled activities and developed an identification inference in

the blockchain. which builds a transaction graph and attempts to deduce node identities using a graph learning approach based on Graph Convolutional Networks. A variety of improvements were also developed by using the unique features of the blockchain transaction graph. Graph Convolutional Network (GCN) is utilized in the model, which is a robust machine learning technique approach intended to operate natively on graphs by using the graph structure as convolutional layers. GCN is significantly improved by including the transaction density information in the graph learning process. Each node in the graph may be represented as a low-dimensional vector, it allows for the visualization of nodes and a good knowledge of classification. It was stated that because the blockchain transaction graph is too complex for traditional graph analytics tools to handle, a graph learning methodology was used to turn the initial graph into a low-dimensional form.

A comprehensive network study of the Bitcoin transaction network was performed in this study by (Tao *et al*. 2022). A unique sampling approach, called random walk with flying-back properties, was developed, and some interesting results were obtained by examining sampled graphs. The degree distribution of the Bitcoin transaction network is indeed a power-law distribution with a large tail, which is close to a scale-free network. By examining the average clustering coefficient, shortest-path length, and small-world measurement, the research determines that the Bitcoin transaction network is a small-world network. The research discovers that most transactions are one-way trades by analysing related components. Furthermore, it was discovered that the Bitcoin network is a multi-centre resilient network against node removal. Following that, due to the Bitcoin network's disassortativity, low-degree nodes prefer joining to nodes with higher degrees. The research also discovered that freshly inserted nodes had a preferred connection. Finally, the existing Bitcoin transaction network does not exhibit the rich-club effect. Such discoveries may aid in a better understanding of the structural characteristics of blockchain networks.

The study by (Thomas N Kipf and Max Welling 2017) reported a scalable method for semi-supervised learning on graph-structured data that is based on an efficient variation of convolutional neural networks that act directly on graphs. The model grows linearly in the number of graph edges and learns hidden layer representations that encode both local graph structure and node attributes by using a localised first-order approximation of spectral graph convolutions. In a series of tests using citation networks and a knowledge graph dataset, we show that our strategy beats similar approaches by a wide margin. The research looks at the challenge of categorising nodes (such as documents) in a graph (such as a citation network) when labels are only accessible for a subset of nodes. This challenge may be framed as graph-based semi-supervised learning, in which label information is smoothed across the network using a graph and some type of explicit graph-based regularisation. The loss function has a Laplacian regularisation term. The study presents a simple and well-behaved layer-wise propagation rule for neural network models that act directly on graphs and demonstrates how it may be explained by the first-order approximation of spectral graph convolutions. The research shows how a kind of graph-based neural network model may be utilised for quick and scalable semi-supervised categorization of graph nodes. Experiments on a variety of datasets show that our model outperforms state-of-the-art semi-supervised learning approaches in terms of classification accuracy and efficiency (measured in wall-clock time). The study presented a unique method for semi-supervised classification of graph-structured data. The GCN model employs an efficient layer-wise propagation rule based on a first-order approximation of graph spectral convolutions. Experiments on a variety of network datasets indicate that the proposed GCN model may encode both graph structure and node attributes in a manner that is suitable for semi-supervised categorization. In this context, the model significantly outperforms numerous previously suggested techniques while being computationally efficient.

TABLE 1. Machine learning-based taxonomic classification of suggested security measures.

Reference	Year	Method	Contribution
(Zambre and Shah 2013)	2013	Machine Learning based Clustering and Classification (KMeans)	Identifying peculiar characteristics of clients exhibiting atypical behaviour by grouping clients with questionable actions.
(Pham 2018)	2016	Unsupervised Machine Learning techniques (KMeans & Graph)	Detection of an anomaly in the bitcoin network where users and transactions are viewed with suspicion.
(Monamo, Marivate and Twala Aug 2016)	2016	Machine Learning based multi-faceted approach (KMeans & Trimmed KMeans)	Bitcoin fraud detection using trimmed k-means and kd-trees, where the fraud is analysed from both a global and local perspective.
(Haohua Sun Yin and Vatrapu Dec 2017b)	2017	Supervised Machine Learning techniques (Gradient Boosting & Bagging)	Show how much of the Bitcoin network is made up of nodes and addresses that are associated with cybercrime and other bad activities.
(Weber 2016)	2018	Machine Learning classifiers and Graphs (Graph Convolutional Network, Random Forest, Logistic Regression and MLP	screening transactions to and from bitcoin wallets to determine the level of risk involved. Each unlabelled Bitcoin transaction must be categorised as either licit or illicit.
(Lihao Nan and Dacheng	2018	Machine Learning and Graph Embedding Techniques	social network analysis using graph embedding and feature-based

Tao Jun 2018)			method to identify mixing services.
(Bartoletti, Pes and Serusi Jun 2018)	2018	Data mining technique	identifying on the network any bitcoin addresses connected to a Ponzi scam.
(Bynagari 2020)	2020	Machine Learning Algorithms (Light Gradient Boosting Algorithm LGBA, XGBoost and Random Forest)	detecting real and fraudulent activity in the financial system at the account and transactional levels
(Liu *et al*. 2022)	2022	Machine Learning and Graph analyses (Graph Convolutional Network)	identity inference in blockchain which builds a transaction graph and uses a graph learning approach based on Graph Convolutional Networks to infer the identities of nodes.

CHAPTER THREE

METHODOLOGY

3.1 Research Methodology

In this section, the architecture of the Bitcoin anomaly detection analysis developed in Figure 1 is explained along with the description of each component. Roughly, the platform analyses the Bitcoin transactions and classifies them in their respective classes, licit transactions or illicit transactions.

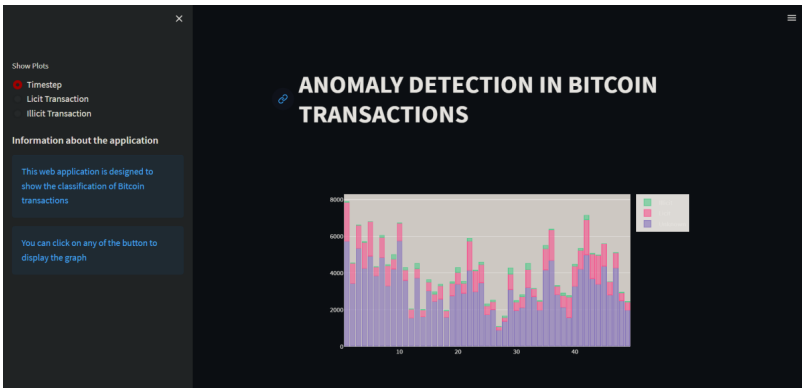


Fig 1 System Architecture

3.1.1 Data Sampling & Collection Method

Although all Bitcoin transaction data is publicly accessible, I would want to stress that data available in relation to heists is minimal. When diving into studying Bitcoin transactions, the significance of this becomes immediately apparent. The presence of mixing services without sufficient information to filter out activities done by these services further complicates the situation. This is due to the fact that the behaviour shown by mixing services could contain characteristic features of robberies.

The Bitcoin graph has a sub-graph that is known as the Elliptic Data Set (Weber 2016). It consists of 234,355 edges and 203,769 nodes in total. In addition to the information on the network, it also classifies the nodes into three classes, namely

"licit," "illicit," and "unknown." The origin of the transaction that corresponds to a node determines whether that node is deemed "licit" or "illicit." The origin of the transaction could be exchanges, wallet providers, miners, financial service providers, etc., or it could be scammers, malware, terrorist organisations, ransomware, Ponzi schemes, etc.

3.1.2 Data Type

Nodes and Edges files: 2% of the nodes are tagged as class1 (4,545) (illicit), while 21% of the edges are categorised as class2 (42,019) (licit). Because so little is known about the other nodes, they are collectively referred to as "unknown." Each node in a particular time step may be seen as an instantaneous "snapshot" in time since their associated time stamps are obviously very near to one another. Over time, the total number of nodes for every time step is nearly uniform (ranging from 1,000 to 8,000 nodes).

Features file: Each node has 166 features that define it, which are known as its description. A time step that ranges from 1 to 49 is used to encode the information on the passage of time. In this stage, the actual time stamp of the transaction is measured. The time steps are equally spaced, with about two weeks between each one. Each of them is composed of a single, interconnected set of transactions that took place on the blockchain within a time span of no more than three hours apart from one another. There are no boundaries between the time steps.

Among them:

- 203,769 nodes (Bitcoin Transactions)
- 234,355 edges (Directed flows)
- 21% licit labels (Known exchanges, wallet providers miners, licit services, etc.)
- 2% illicit labels (Known scams, malware, terrorist organizations, ransomware, Ponzi schemes, etc.)
- 94 local features (LF) e.g., time step, in / out count activity, transaction fee.
- 72 one-hop aggregate feature (AF) (e.g., max, min standard deviation, and correlation coefficients of the nearest transactions
- Size on disk 146mb (Compressed Zip file)

3.1.3 Features dataframe explanation:

- The transaction id is located in the first column, which has the name 0.
- Timesteps are displayed in column 1, which corresponds to each node. These timestamps are separated by a period of two weeks. Each timestamp includes a related component of transactions that were added to the blockchain less than three hours apart from one another between each other.
- Next 93 features display information regarding the transaction, including the number of inputs and outputs, the transaction fee, the output volume, and aggregated figures such as the average BTC received (spent) by the inputs and outputs and the average number of incoming (outgoing) transactions associated with the inputs and outputs.
- The remaining 72 features are aggregated features that were acquired by using transaction information one-hop backward/forward from the centre node. These features give the maximum, minimum, standard deviation, and correlation coefficients of the neighbouring transactions for the same information data (number of inputs/outputs, transaction fee, etc.).

3.1.4 Analysis Technique

Using this data, transactions to and from cryptocurrency wallets will be screened to determine the risk involved in each transaction. Given a set of features and the network architecture, each unlabeled Bitcoin transaction must be classified as either licit or illicit. Because not all of the nodes are labelled, the problem may alternatively be resolved in a semi-supervised context that takes into consideration the data carried by the unlabelled nodes. When developing functionality for Bitcoin transactions, one of the most significant obstacles researchers encounter is the fundamental requirement to access the entire blockchain. This is necessary in order to view the complete history of wallets that took part in the transactions that were chosen. The second difficulty stems from the underlying graph structure of the data and the variability in the number of neighbours that a transaction may have. Both of these factors contribute to the first difficulty. By naively producing statistical aggregates (minimum, maximum, etc.) of the local features of a neighbour transaction, the issue of heterogeneous neighbourhoods is addressed in the process of building the 72 aggregated features. In general, this technique is not ideal because it results in a sizeable loss of information, which might be considered significant. a more accurate representation of the local graph topology is graph deep learning.

3.2.1 The Case for Graph

It is possible to show the network of the bitcoin blockchain using a variety of various approaches. The nodes in the graph indicate transactions, and the edges illustrate how bitcoins travel from one event to the next. This makes the graph one of the most straightforward possible to illustrate bitcoin network. A Directed Acyclic Graph (DAG) network is shown here as fig 1.0's representation of the blockchain for bitcoin transactions. The number of inputs that a transaction requires is indicated by a node's in-degree, and the number of outputs that a transaction requires is indicated by a node's out-degree, with the exception of

rare circumstances (when a number of outputs from one transaction are subsequently utilised as inputs in another transaction).

A timestamp is affixed to each transaction and serves as a representation of the approximate time at which the transaction was sent to the Bitcoin network. This makes it possible to include time information into the visualisation of a graph. Anyone who operates a Bitcoin node has access to every transaction that is recorded on the blockchain and can consequently generate the full graph based on those transactions. The graph that represents all of Bitcoin's transactions has more than 1.1 billion edges and 438 million nodes. The graph is continually growing as a result of the fact that there are more than 350,000 newly validated bitcoin transactions taking place every day.

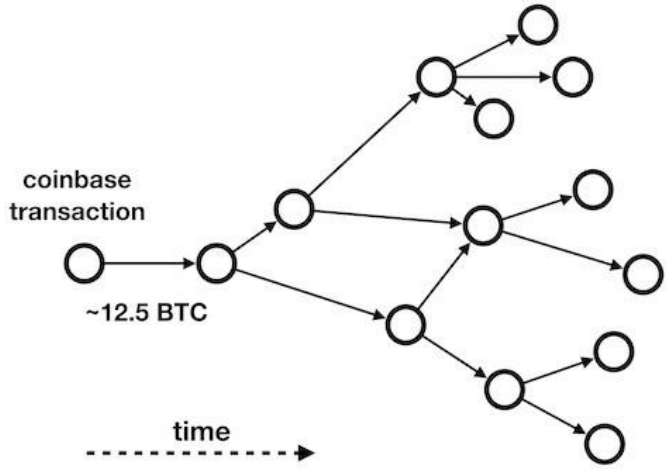


Fig. 1 — DAG that a coinbase transaction initiated. Transactions are represented by nodes, and time goes from left to right.

In recent years, graph analysis has attracted a growing amount of attention, which has enabled researchers to study the various network systems in a more methodical approach. Graph learning is an efficient method that can be used to

find a solution to the problem of graph analytics. This method turns the graph into a low-dimensional space while still maintaining the integrity of the graph's information. It is abundantly evident that the graphs representing bitcoin transactions are rather sparse, and these graphs may be subdivided into a number of different subgraphs. The edge density is relatively high inside each component, but it is low amongst various components.

The local features in the Elliptic Data set have been improved by the addition of a set of 72 features, each of which includes information regarding the immediate neighbourhood. Features. Exploitation of these features results in an increase in performance. Despite the fact that this method demonstrates that the network structure is relevant to the binary classification problem and that it is possible to apply standard machine learning techniques to this, Extending the solely feature-based strategy outside the immediate neighbourhood presents a number of difficult challenges. This limitation is what drives the development of Graph Convolutional Networks.

3.2.2 Autoencoders

The process of encoding something automatically is what is meant to be understood by the term "autoencoder." The autoencoder is able to learn how to breakdown data, which in our instance pertains to the detection of credit card fraud, into very little bits of data. It is then able to use that depiction to recreate the original data as closely as it can to the original.

There are two primary parts that make up an Autoencoder:
Encoder: learns how to reduce the original input into a tiny encoding, The purpose of the encoder is to discover the shortest feasible representation of the data that it can retain. This entails selecting the most salient features of the original data and encoding it in a manner that the decoder can comprehend.

Decoder: Figures out how to get the data in its original form from the encoding that was produced by the Encode command. The Decoder operates in a manner that is similar to that of the Encoder, but in the opposite direction. Instead of creating, it develops its reading skills. The dataset is scaled and separated into licit and illicit cases.

3.2.3 Building the Autoencoder Model

Autoencoders are a specialized subcategory of neural network architectures in which the output is identical to the input. In order for autoencoders to learn the very low-level representations of the input data, they are trained in an unsupervised way. The projected real data is then created by deforming these low-level characteristics back into their original shape. An autoencoder is a kind of regression in which the network is asked to make predictions about its own input (in other words, model the identity function). Because these networks have a constrained bottleneck in the centre consisting of just a few neurons, they are compelled to provide efficient representations that reduces the input into a low-dimensional code. The decoder may then utilise this code to replicate the input as it was originally received.

3.2.4 Model Training

The model will be trained from 4000 separate licit transactions throughout the training process. We do not need an excessively large number of data samples in order to acquire the appropriate representations. The autoencoder will only be trained on a total of 4000 rows, each representing a licit transaction. In addition, there is no need to execute this model for a significant number of epochs.

3.2.5 Finding Latent Representations

After the model has been trained, a latent representation of the input learnt by the model is obtained. the trained model's weights provide access to this. Another network with sequential layers is built, only adding trained learned weights until the third layer, when latent representation exists. Using the model to predict the raw inputs to generate the hidden representations of two classes: licit and illicit. Then, using the latent representations collected, a dataset was generated to show the nature of illicit versus licit cases.

3.3 Models

The distance between certain seed nodes and known illicit nodes is specified, and the performance of features produced from a The distance between particular seed nodes and known illegal nodes is determined, and the effectiveness of classification task features is evaluated. Feature extraction is conducted initially after successful random walks. The training and test data are then split 70/30, and the results are compared using various classification models that make use of all of the original features in the dataset.

Anomaly detection in Bitcoin transactions has employed graphs, Supervised and Unsupervised machine learning models. According to (Weber 2016), Logistic Regression and Random Forest are two benchmark approaches for anomaly dedection, and Graph Deep Learning has emerged as a potential tool as well. They used Random Forest, Logistic Regression, and a Multi-Layer Perceptron classifier. A Random Forest, in essence, selects a subset of features at random in order to build a decision tree with the best split across its nodes, where multiple trees are created to create an ensemble of decision trees, and it use a voting mechanism to ensemble the predictions made by many decision trees, each of which was trained on a subset of the data.

(Monamo, Marivate and Twala Aug 2016) emphasised that trimmed KMeans clustering yielded excellent results with improved detection rate for known illicit transactions. Although (Pham 2018) reiterated that k-means clustering is not a reliable tool for detecting outliers while (Monamo, Marivate and Twala Aug 2016) implies that KMeans provides a foundation for evaluating approaches. Outliers will be located furthest from the centroids of clusters with which they are related. Gradient boosting use a sequence of trees as a weak classifier to produce a strong classifier using gradient descent. (Haohua Sun Yin and Vatrapu Dec 2017) used the Gradient Boosting technique was utilised on the cybercrime-related categories in the research based on their weighted average and per class precision. To reach its outcome, the voting classifier employs a hard-voting strategy.

CHAPTER FOUR

RESULTS

4.1 Experimental outcome

The outcomes of the experiment are presented in this section. A temporal split of 70:30 between the training data and the test data was performed. The model was trained using 4,000 different examples of licit transactions, it is now able to recognise illicit transaction occurrences. As a result, experiments were performed on the standard classification models for the licit/illicit prediction using a variety of standard and ensemble method approaches. These included Logistic Regression, K Nearest Neighbors, Decision Tree Classifier, Random Forest, XGBoost, Gradient Boosting, Multi Layered Perception, and Extra Trees (with default parameters from the scikit-learn Python package).

The hyperparameter tuning for Logistic Regression with C value of 10. Random Forest with maximum tree depths of 50, maximum tree counts of 50, and maximum feature counts of 5. XGBoost with 500 numbers of trees, 50 maximum depths, and a learning rate of 0.1, Gradient Boosting with a learning rate of 0.1, and Extra Tree with 50 numbers of trees. When analysing these models, each of their 166 attributes was taken into consideration. The findings are summed up in Table 2, which may be seen below.

S/N	Model	Precision	Recall	F1-Score	AUC-Score
1	Logistic Regression	96%	95%	96%	95%
2	KNN	96%	96%	96%	96%
3	Decision Tree	92%	94%	93%	93%
4	Random Forest	99%	94%	96%	96%
5	XGBoost	98%	96%	97%	97%
6	Gradient Boosting	97%	96%	96%	96%
7	MLP	97%	97%	97%	97%
8	Extra Trees	98%	94%	96%	96%

Table 1: Model Evaluation Metrics Table

CHAPTER FIVE

DISCUSSION

5.1 Results of classifications machine learning algorithms

As shown in Table 1 above, The models with the best performance are Random Forest, XGBoost, and Extra Trees. The use of Autoencoder has been effective in resolving the issue of class imbalance in the dataset, and the utilisation of ensemble learning in conjunction with Voting Classifier has enabled the development of the most accurate model possible. It became clear that the supervised learning algorithms had achieved similar results as the original research's suggested model on the Bitcoin dataset. That was done in the original study presented by (Weber 2018). The Voting Classifier has attained an accuracy of 97.50% compared to the accuracy of the 97.70% accuracy from the Random Forest model to classify the Bitcoin dataset using all 166 features.

5.2 Dataset limitation

The dataset that was used in this study has a few limitations. To begin, there are certain classes that were significantly oversampled while others were significantly undersampled (see Figure 1). There are less than 10 instances in categories like stolen bitcoins and mixing., which may explain why the models don't perform well when predicting mixing. While there are over 200 observations for both personal wallets and exchanges.

CONCLUSIONS

According to the findings of the research that was carried out, random forest was the technique that performed the best when compared to the other options when it came to recognizing fraudulent transactions in the Bitcoin dataset. Using autoencoders as a tool, this study conducts an examination into the problem of class imbalance that is present in the dataset. In addition to the studies that are presently being carried out, the model could be able to assist in the process of detecting entities that are likely involved in fraudulent activity. As a future work, the plan is to combine this approach with other methods such as Graph Convolutional Network to develop a more robust anomaly detection tool in view of the future emergence of new methods developed to aid fraudulent transaction in the financial infrastructure as a whole. This will be done with the intention of developing a more robust anomaly detection in view of the future emergence of new methods developed to aid fraudulent transaction in the financial system.

RECOMMENDATION

To deanonymize Bitcoin transactions and access to publicly accessible data, additional info about true fraudulent transactions should be made publicly available from financial institutions to researchers. Further research and development should be dedicated in this area. Combinations of graph embedding methods with machine learning strategies that do not suffer from the limitations of a lengthy computational run time.

REFERENCE LIST

BARTOLETTI, M. *et al.*, 2021. Cryptocurrency Scams: Analysis and Perspectives. *IEEE access*, 9, 148353-148373

BARTOLETTI, M., B. PES and S. SERUSI, Jun 2018. Data Mining for Detecting Bitcoin Ponzi Schemes. IEEE, pp.75-84

BYNAGARI, N.B., 2020. The Difficulty of Learning Long-Term Dependencies with Gradient Flow in Recurrent Nets. *Engineering International*, 8(2), 127-138

CUNEYT GURCAN AKCORA, YITAO LI, YULIA R GEL and MURAT KANTARCIOGLU, 2019. *BitcoinHeist: Topological Data Analysis for Ransomware Detection on the Bitcoin Blockchain.* Ithaca: Cornell University Library, arXiv.orgAvailable from: https://search.proquest.com/docview/2243849112

D'ORO, P., *et al.*, *Group Anomaly Detection via Graph Autoencoders*.

HAOHUA SUN YIN and R. VATRAPU, Dec 2017a. A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning. IEEE, pp.3690-3699

HIRSHMAN, J., Y. HUANG and S. MACKE, *Unsupervised Approaches to Detecting Anomalous Behavior in the Bitcoin Transaction Network*.

LIHAO NAN and DACHENG TAO, Jun 2018. Bitcoin Mixing Detection Using Deep Autoencoder. IEEE, pp.280-287

LISCHKE, M. and B. FABIAN, 2016. Analyzing the Bitcoin Network: The First Four Years. *Future Internet*, 8(4), 7

LIU, X. *et al.*, 2022. A Graph Learning Based Approach for Identity Inference in DApp Platform Blockchain. *IEEE transactions on emerging topics in computing*, 10(1), 438-449

MONAMO, P., V. MARIVATE and B. TWALA, Aug 2016. Unsupervised learning for robust Bitcoin fraud detection. IEEE, pp.129-134

NERURKAR, P. *et al.*, 2021. Dissecting bitcoin blockchain: Empirical analysis of bitcoin network (2009–2020). *Journal of Network and Computer Applications*, 177, 102940

NICHOLLS, J., A. KUPPA and N. LE-KHAC, 2021. Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. *IEEE access,* 9, 163965-163986

PHAM, T.T., 2018. Collective Anomaly Detection: Application to Respiratory Artefact Removals. *Applying Machine Learning for Automated Classification of Biomedical Data in Subject-Independent Settings*. Cham: Springer International Publishing, pp.49-81

RAHOUTI, M., K. XIONG and N. GHANI, 2018. Bitcoin Concepts, Threats, and Machine-Learning Security Solutions. *IEEE access,* 6, 67189-67205

RAO, S.X. *et al.*, 2021. xFraud. *Proceedings of the VLDB Endowment,* 15(3), 427-436

TAO, B. *et al.*, 2022. Complex Network Analysis of the Bitcoin Transaction Network. *IEEE transactions on circuits and systems. II, Express briefs,* 69(3), 1009-1013

THOMAS N KIPF and MAX WELLING, 2017. *Semi-Supervised Classification with Graph Convolutional Networks*. Ithaca: Cornell University Library, arXiv.orgAvailable from: https://search.proquest.com/docview/2075308524

WEBER, B., 2016. Bitcoin and the legitimacy crisis of money. *Cambridge journal of economics,* 40(1), 17-41

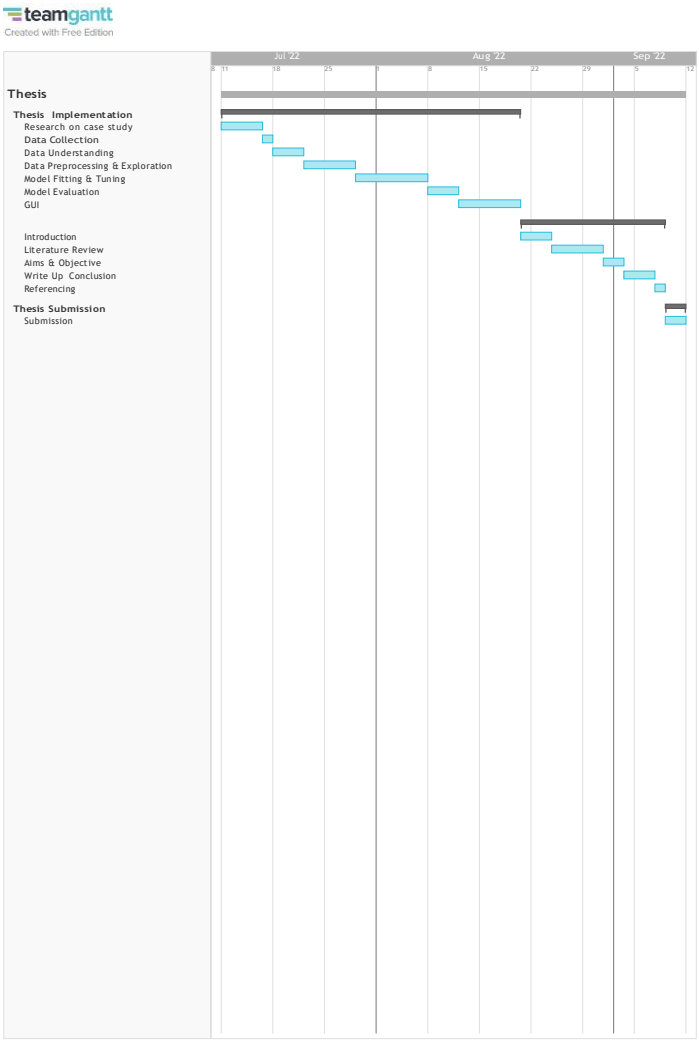
WU, J. *et al.*, 2022. Detecting Mixing Services via Mining Bitcoin Transaction Network With Hybrid Motifs. *IEEE transactions on systems, man, and cybernetics. Systems,* 52(4), 2237-2249

YINING HU, SURANGA SENEVIRATNE, KANCHANA THILAKARATHNA, KENSUKE FUKUDA and ARUNA SENEVIRATNE, 2019. *Characterizing and Detecting Money Laundering Activities on the Bitcoin Network*. Ithaca: Cornell University Library, arXiv.orgAvailable from: https://search.proquest.com/docview/2331355699

ZAMBRE, D. and A. SHAH, 2013. *Analysis of Bitcoin Network Dataset for Fraud.*

Appendices

Project Plan



Graphics User Interface