Anonymity Analysis of Bitcoin Transactions Using Unsupervised Machine Learning

Bivin S. Nair, Regi Kumar V.

Financial Engineering, Department of Mechanical Engineering, College of Engineering, Trivandrum, Kerala, India

Abstract- **Bitcoins are digital currencies that works on technology called blockchain, which is a public electronic ledger that is openly shared among the nodes in the network and creates an unchangeable record of the transactions. In financial networks, thieves and their illegal activities are called as anomalies. Members of a network want to detect anomalies as soon as possible to prevent them from creating problems in the network's community and integrity. This study focuses on anomaly detection of the bitcoin transactions using unsupervised machine learning method. An anomaly detection model is developed with the help of isolation forest algorithm. The developed model initially extracts all bitcoin transaction data and various features of the same. The incorporated isolation forest algorithm isolates observations by arbitrarily choosing a feature and afterward split the value amongst most extreme and least ones of the selected features. The anomalies are detected by running developed the isolation forest model and the most suspicious transactions are determined for corrective action.**

Keywords: **Bitcoin, Anomaly, Financial Transaction, Clustering, Isolation Forest**

I. INTRODUCTION

Bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem. Units of currency called bitcoins are used to store and transmit value among participants in the bitcoin network. Bitcoin users communicate with each other using the bitcoin protocol primarily via the Internet, although other transport networks can also be used. The bitcoin protocol stack, available as open source software, can be run on a wide range of computing devices, including laptops and smartphones, making the technology easily accessible.

Bitcoin is the name of the protocol, a peer-to-peer network, and a distributed computing innovation. Bitcoin represents the culmination of decades of research in cryptography and distributed systems and includes four key innovations brought together in a unique and powerful combination. Bitcoin consists of:

- A decentralized peer-to-peer network (the bitcoin protocol)
- A public transaction ledger (the blockchain)
- A set of rules for independent transaction validation and currency issuance (consensus rules)
- A mechanism for reaching global decentralized consensus on the valid blockchain (proof-of-work algorithm)

The total volume of bitcoin that can be mined is limited to 21 million after that no more bitcoins can be mined or created. The volume of coins that can be mined is controlled by the built in algorithm designed in the bitcoin protocol. The mathematical problem will be gradually harder when a certain limited is reached, which is known as controlled supply. Until now almost 17 million bitcoins are mined which is about 81% of the total amount of mined coins.

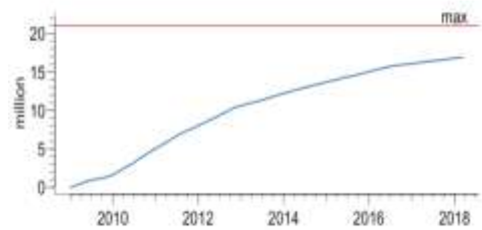

Figure1.1: Bitcoin Growth (2008-2018)

1.1 Bitcoin Transactions

A transaction is the basic operation in the Bitcoin system. A Bitcoin transaction moves bitcoins between one or more inputs and outputs. Each input is a transaction and address supplying bitcoins. Each output is an address receiving bitcoin, along with the amount of bitcoins going to that address

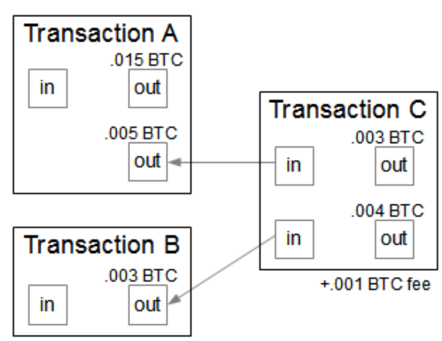

Figure1. 2: Sample Transaction

Figure 1.2 depicts a sample transaction 'C'. In this transaction, 0.005 BTC are taken from an address in the transaction A, and 0.003 BTC are taken from an address in transaction B. For the yields, 0.003 BTC are coordinated to the primary address and 0.004 BTC are coordinated to the second address. The remaining 0.001 BTC goes to the miner of the block as an incentive. Note that the 0.015 BTC in the other yield of Exchange A isn't spent in this exchange.

1.2 Consensus in Blockchain

Blockchain are **public, decentralized** database that keeps public records. When the data are added into the blockchain it cannot be customized and is very difficult to fake entries. This type of feature is termed as **persistence**. When new data needs to be updated, the record must be added to the existing information. Any entry in the database can be viewed by any person who is a member and also can check the authenticity of the transactions. This is why block chains are said to be auditable**.**

The main consensus in a blockchain are the practical byzantine fault tolerance algorithm (PBFT), the proof-of-work algorithm (PoW) ,the proof-of-stake algorithm (PoS), and the delegated proof-of-stake algorithm (DPoS).

1.2.1Practical Byzantine Fault Tolerance Algorithm (PBFT)

All validation nodes keep open connection to each other. One can submit their transaction to any of them, and this transaction will be broadcasted to other nodes in the network. One node is elected as a leader. At the moment when a new block is going to be generated:

i. The leader orders the transactions that should be included in a block, and broadcasts this list of ordered transactions to all other validation nodes in the network.
ii. When each of the validation nodes receives the ordered list of transactions, each validation nodes does the following:
   a) It starts executing the ordered transactions one by one.
   b) As soon as all the transactions are executed, it will calculate the hash code for the newly created block.
   c) Then it broadcasts its answer (the resulting hash code) to other nodes in the network, and starts counting the responses from them.
   d) If 2/3 of all validation nodes have the same hash code, it will commit the new block to its local copy of the ledger.

1.2.2 Proof-of-Work (PoW)

Bitcoin uses proof- of - work method for attaining consensus on a blockchain. Compared to the PBFT, PoW does not require all nodes to submit their individual conclusions to reach the consensus. In PoW technique, hash function is utilized to make conditions by which each clients are allowed to communicate their decisions about the submitted data, and the conclusions would then be able to be freely confirmed by every single other client in the system. The advantage of hash function is false conclusions are avoided by the parameters of the hash and their by ensuring that false data will neglect to register in a satisfactory way.

The users who verify the information in the network are rewarded for their participation with newly mined bitcoins. This process of searching for valid hashes is known as mining. Incentivizing the users for the participation in the blockchain network ensure broad participation, which results in more robust network and a safer blockchain.

1.2.3 Proof-of-Stake (PoS) Algorithms

The proof-of stake algorithm is similar to the proof-of-work system, but the difference is that in PoS algorithm the hash function is replaced by digital signature which proves the ownership of the stake. Based on the relative stake in the network, the nodes randomly select a user to approve newly added transactions. The bitcoin uses the PoW consensus algorithm and the PoS consensus algorithm is used by the organization known as peercoin. Bitcoin participants are incentivized with bitcoin; likewise peercoin also provides incentives to participants, who ensure broadest networks and its security. In the PoS system, the chosen party is rewarded with a new Peercoin through a process called minting. Therefore the participants of PoS systems have put forward a number of various modifications to ensure that the network remains broad as possible.

1.2.4 Delegated Proof-of-Stake (DPoS) system

The delegated **proof-of-stake (DPoS) system** is almost similar to that of the PoS system, except that individual users choose the most important entity to represent their portion of stake in the network. The users with smaller stake of ownership joints together to magnify their representation which will result in the balance of power compared to large stake holders.

1.3 Literature Review

Duen Horong [1] and Adam wright introduce a calculation based on belief network algorithm to induce records to make inferences on hailing documents with low notoriety as malware. They ran the tests on a large graph consisting of 1 billion nodes and 37 billion edges. Nodes comprised of machines and records in a bipartite system. They appear, in light of exact information from their tests, that the Polonium calculation is compelling in enhancing exactness in recognizing malware. Fergal Reid [2] and Martin harrigan described that users who tries to attack will try to create too many mapping between the users and public keys and will correlate information external to the system with the users. This considered the topological structure of the two networks obtained from the Bitcoin public transaction history. Gross [3] and Acquisiti discuss privacy of early users in the facebook social network, and how information from multiple sources could be combined to identify pseudonymous network users. Narayanan and Shmatikov [4] consider privacy attacks which identify users using the structure of networks and show the difficulty in guaranteeing anonymity in the presence of network data. Puzis et al.[5] simulated the monitoring of a communications network using strategically-located monitoring nodes and showed that, using real-world network topologies, a relatively small number of nodes can collaborate to pose a significant threat to anonymity. Y.Altshuler et al. [6] talk about the expanding perils of assaults focusing on comparative kinds of data, and give measures of the trouble of such assaults, on specific systems. The majority of his work focuses to the trouble in keeping up namelessness where organize information on client conduct is accessible and outlines how apparently minor data leakages can be totaled to posture critical dangers.

1.4 Methodology and Data Analysis

The methodology adapted to build the detection model is shown in figure 1.3, in which design of the system is depicted.

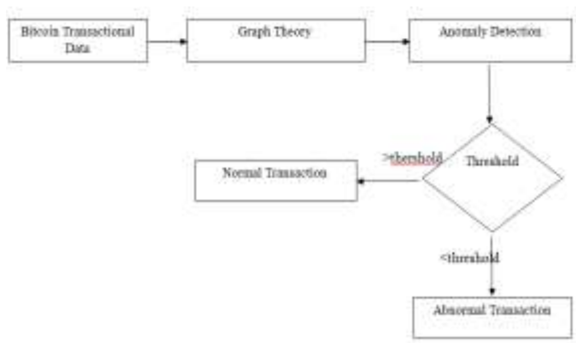

Figure 1.3: Work flow Diagram

1. Bitcoin Transactional Data

The Bitcoin Transactional data is downloaded from the selected authentic site [12].Each transaction consists of:

1. User ID sending bitcoin.
2. User ID receiving bitcoin.
3. Amount of bitcoin transferred.
4. Date and time when the transaction occurs.

2. Graph Theory

Transaction in a financial system forms a graph where each user is the node and each transaction is an edge. The graph theory will be useful in analyzing transaction and finding anomalies. The aim is to extract the features from the bitcoin transactional datasets that will segregate rouge users from good users. The features are described below:

- User in degree: represents the number of incoming transactions to a user.
- User out degree: represents the number of outgoing transactions from a user.
- User unique in degree: represents the number of unique users from which the user has received bitcoin.
- User out degree: represents the number of unique users to which a user has sent bitcoin.
- In-transaction rate: represents the outgoing transaction frequency for the user.
- Out-transaction rate: represents the outgoing transaction frequency for the user.

3. Anomaly Detection

Anomalies are detected using Isolation forest Classifier. A robust algorithm for detecting anomalies. The algorithm is based on the fact that anomalies are data points that are few and different and does not require assumption on data. Isolation forest forms a tree which randomly split data into different partitions until every point is isolated. The data point located at leafs with shorter path from the roots are likely to be the outliers. Using the extracted features the outliers are determined from the bitcoin transaction datasets.

4 Threshold Value

After running the isolation forest model a threshold value is obtained. The transactions below the threshold values are abnormal transactions and the transaction above the threshold values are normal transactions. The plot for the normal and abnormal transactions is visualized using python packages.

5. Isolation Forest (IF) for Anomaly Detection

Isolation Forest (IF) comprises of a set of t trees denoted by $T = \{T1, ...,Tt\}$ constructed in a randomized manner .Each tree is constructed from the root to leaves by randomly partitioning the data at each node by selecting a feature and a threshold both at uniformly random. The trees are grown until each instance is isolated in a leaf. IF is based on the idea that anomalous instances are few, and they are well-separated from clusters of nominal instances in the feature space. Because of this, anomalous instances very quickly reach leaf nodes through random partitioning. On the other hand, nominal instances, which form dense clusters, require many more splits to finally reach leaf nodes. Therefore, the length of the path traversed by an instance from the root node to the leaf, also known as the isolation depth, is shorter (on average) for anomalous instancesthan it is for nominal instances. The anomaly score assigned to an instance is simply the average isolation depth across the forest. It is straightforward now to describe IF as a particular way of setting the weights of a tree-based anomaly detector. In particular, the weight of each node v is $w_v = -1$ (constant). Given an instance x, it is easy to see that the anomaly score assigned by the tree-based detector is simply negative of the average number of nodes on paths traversed by x in the forest, i.e. negative of the average isolation depth. Note that, the main purpose to make scores negative is to ensure that higher scores indicate more anomalous and lower scores indicate more nominal.

1.5Results and Discussions

On running the isolation forest model for 10,48,576 transactions, 10,553 transactions are found abnormal. The model found transaction with an anomaly score -0.21385 or lower where categorized as anomalies. The normal and abnormal transactions are shown in figure 1.4, with blue dots as normal transactions and red dots as abnormal transactions.

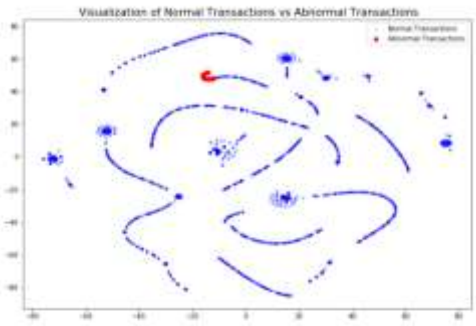

Figure1.4: Normal Vs Abnormal Transactions

The figure 1.4 shows the t-sne visualization of Normal Transaction and abnormal transactions. t-sne is a diamensionally reduction technique to visualize high dimension data.

- The dataset consists of 10,48,576 transactions of that 10,553 are abnormal transactions.
- Using the directed graph, strongly connected components are identified, which is the most suspicious transactions.
- Transactions 9, 18, 31, 264431, 288084, 812872 are found to be most suspicious.

II. CONCLUSIONS

This study focuses on detection of the anomalous transactions in the bitcoin network. Bitcoins are virtual currencies which are used for buying and selling goods, transfer money to individuals or firms. For detecting anomalies a model is developed using isolation forest classifier, then predict the anomalies in the transaction data. From a selective authentic site the datasets are downloaded. The dataset consists of 10, 48,576 transactions. After running the model 10,553 transactions were found abnormal that is approximately 1% anomalous transactions. The normal and abnormal transactions are visualized using t-sne python packages. The t-sne packages are useful in detecting high dimensional dataset. Using the network packages the directed graphs and multi directed graphs are constructed. The strongly connected components from the directed graph are identified which determines the suspicious transactions

III. LIMITATIONS AND FUTURE WORK

The main limitations of the study are systems with more computational power is required, minimum 8GB ram is required. Since the dataset set are large and complicated only limited features are extracted to detect the anomalies. In this project only limited features are extracted to detect the abnormal transactions. With more informative feature extraction, it might be able to explore more suspicious behaviour in the network.

REFERENCES

[1]. Duen Horng (Polo) Chau, Carey Nachenberg, Jeffrey Wilhelm, Adam Wright, Christos Faloutsos Polonium: Tera-Scale Graph Mining and Inference for Malware Detection 2011, Proccedings of SIAM International Conference on Data Mining (SDM).

[2]. Reid, F. and Harrigan, M. An Analysis of Anonymity in the Bitcoin System 2011

[3]. R. Gross and A. Acquisti. Information Revelation and Privacy in Online Social Networks. In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, pages 71-80. ACM, 2005.

[4]. Narayanan and V. Shmatikov. De-anonymizing Social Networks. In Proceedings of the 30th Symposium on Security and Privacy.

[5]. R. Puzis, D. Yagil, Y. Elovici, and D. Braha. Collaborative Attack on Internet Users Anonymity. Internet Research, 19(1):60-77, 2009.

[6]. Y. Altshuler, N. Aharony, Y. Elovici, A. Pentland, and M. Cebrian. Bitcoin: An Innovative Alternative Digital Currency. Hastings Science& Technology Law Journal.

[7]. Farren, D., Pham, T., and Alban-Hidalgo, M. Low LatencyAnomaly Detection and Bayesian Network Prediction of Anomaly Likelihood. arXiv preprint arXiv:1611.03898, 2016.

[8]. Pham, T. and Lee, S. Anomaly Detection in the Bitcoin System - A Network Perspective. arXiv preprintarXiv:1611.03942, 2016.

[9]. Adrian Blundell-Wignall. The bitcoin question: Currency versus trustless transfer technology. OECD Working Papers on Finance, Insuranceand Private Pensions, 2014.

[10]. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Consulted, 1(2012):28, 2008.

[11]. Deepak Zambre and Ajey Shah. Analysis of bitcoin network datasetfor fraud. Unpublished Report.

[12]. http://anonymity-in bitcoin.blogspot.com