Fraud Detection in Cryptocurrency Transactions

Jeet Gupta **Rishabh Narayanan** **Tri-An Nguyen** **Khyaati Sigicherla** **Veda Yakkali**

1 Overview

In this project, we aim to explore and develop methods for visualizing and predicting fraudulent transactions in cryptocurrency (crypto), with a focus on BitCoin. The decentralized and immutable nature of crypto creates greater pseudonymity for fraudsters but also enables much larger scale forensic analysis for fraud detection. Being a nascent field, newer techniques for both evasion and detection are constantly being developed. In this project, we hope to employ machine learning techniques to predict fraud on a semi-supervised dataset.

2 Dataset

We have a candidate dataset to explore from a previously published paper. Weber, et al. (2019) published the Elliptic dataset while exploring graph convolutional networks for fraud detection [1].

Interestingly, the dataset represents transactions as graphs and includes a core temporal aspect. Specifically, the Elliptic Dataset includes a graph transaction dataset with V=203,769 and E=234,355. There are 166 features including a time step that represents when transactions were made, which is useful in detecting the fraudulent moving of money between accounts [1].

This dataset is partially labeled with heavy class imbalance necessitating the development of robust semi-supervised techniques. Roughly 2% of the dataset is labeled as ilicit (N=4,545), 21% of the dataset are licit transactions (N=42,019), and the remaining 77% (N=157,205) are unknown [1].

3 Visualization

One goal of our project is to develop better ways to visualize the high dimensional, temporal, and graphical aspects of the transactions dataset. High dimensionality necessitates dimensionality reduction techniques like Principal Component Analysis (PCA) or Uniform Manifold Approximation and Projection (UMAP), and the temporality and graphical nature introduces additional visualization complexities. We want to explore if visualizations alone will indicate any interesting discriminatory behaviors between licit and illicit transactions.

4 Fraud Prediction

4.1 Supervised

A second important goal of our project is to develop robust predictive models to discriminate fraudulent transactions. Weber, et al. (2019) explored models like Random Forest (RF), Multi-Layered Perceptrons (MLP), and Graph Convolutional Networks (GCN) [1, 2], and found that RF performed the best [1]. We would like to validate this model and evaluate other models like Support Vector Machines (SVM) or maybe more time-aware models like Cox regression.

4.2 Unsupervised

We also plan on developing unsupervised anamoly detection models like Isolation Forests since they do not need labeled data. The majority unlabeled portion of our dataset suits unsupervised or

semi-supervised techniques better. The labeled portions can instead be used for validation and model scoring.

Another idea we had was to build a Variational Autoencoder that aims to compress the high dimensional dataset into a smaller dimensional latent space before reconstructing the original [3]. In doing so, we hope that minor inconsistencies in fraudulent transactions would be better emphasized as anomalies. We are unsure whether such a model is feasible to build given our timeline, but we would like to explore it if time permits.

4.3 Evaluation

We shall evaluate all models we decide on using using metrics like accuracy, F1 scores, and ROC curves. For unsupervised techniques, we shall use the labeled datapoints to measure cluster spread, precision, and recall of the known illicit transactions. If time permits, we will attempt hyperparameter tuning with K-fold cross validation. We shall compare our various models and visualizations to understand which models are most predictive of fraud.

5 Challenges

The nature of the dataset presents numerous challenges. The dimensionality itself creates issues with sparsity and issues with overfitting. Effective feature reduction techniques will be crucial to implement. Moreover, the graph nature of the dataset with nodes and edges is not ideal to represent in matrix form. We need to brainstorm better ways of representing our data for each of machine learning. The semi-supervised nature also limits certain methods that we may use, with the class imbalance requiring greater attention to prevent class bias.

The temporal aspect also introduces complexities as transactions are not point-in-time events. Money laundering is typically achieved by wiring BitCoin in complicated ways that become difficult to trace. An additional challenge is that the dataset is limited to transactions between 2009-2018. Fraud and crypto has greatly evolved since, and newer techniques would need to be developed for modern detection.

6 Summary

In conclusion, we hope to investigate visualization and predictive techniques to answer some of the following research questions. 1) Which methods (supervised/unsupervised) have the greatest predictive power. 2) Which features are most predictive of fraud. 3) How does temporality affect model performance on older versus recent transactions.

References

[1] Weber, M., Domeniconi, G., Chen, J., Weidele, D. K. I., Bellei, C., Robinson, T., & Leiserson, C. E. (2019). Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics.

[2] Asiri, A., & Somasundaram, K. (2025). Graph convolution network for fraud detection in bitcoin transactions. Sci Rep 15, 11076.

[3] Koronaios, A., & Koloniari, G. (2025). Graph-Based Bitcoin Fraud Detection Using Variational Graph Autoencoders and Supervised Learning. Procedia Computer Science, 257, 817–825.