A Multi-Feature Fusion Based Method for Detecting Illicit Bitcoin Transactions

JIANG Xianbo, KANG Yanrong, XING Guidong, GUO Lili, ZHANG Qian, ZHANG Yaoguo, BAO Menghu, ZHAO Lu, WANG Bo, NIE Leihang, LIU Shuqi, ZHANG Qingpu, CHU Chuanhong

Institute of Forensic Science, Ministry of Public Security (MPS), Beijing 100038, China

Abstract

Bitcoin's pseudo-anonymity facilitates illicit activities[1] such as money laundering, terrorist financing, and illegal goods trading, posing significant challenges to **blockchain regulation and digital forensics.**

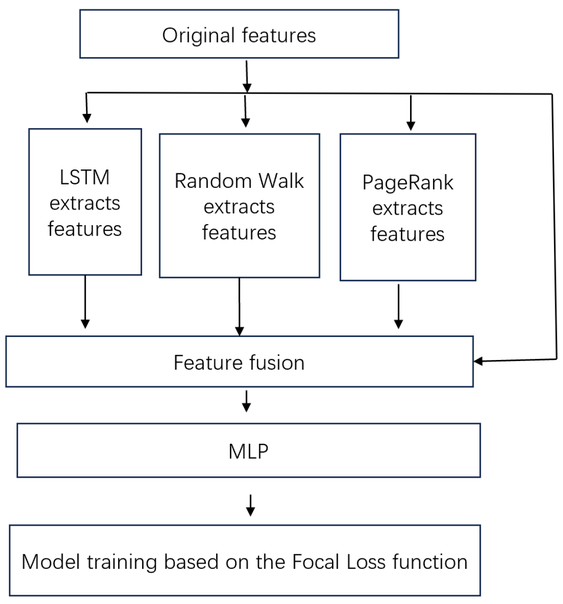
To address limitations in existing detection methods—particularly **insufficient feature representation and extreme class imbalance**—this work proposes **a multi-feature fusion framework for illegal Bitcoin transaction detection**.

The model integrates **traditional transaction attributes with temporal features extracted by LSTM**[2], **structural proximity features derived from Random Walks**[3], and **global importance indicators based on PageRank**[4], enabling a **comprehensive characterization of transaction behaviors**.

Experiments conducted on the Elliptic dataset[5] demonstrate that the proposed approach achieves **competitive performance under highly imbalanced conditions,** outperforming several mainstream graph-based and neural network baselines in terms of detection effectiveness.

The proposed framework provides practical support for **blockchain-based digital forensics and law enforcement investigations**, particularly in **prioritizing suspicious addresses, tracing illicit fund flows, and assisting investigators during early-stage case screening**. By improving detection performance under severe class imbalance, the approach helps **reduce manual analysis effor**t and **enhance investigative efficiency** in real-world cryptocurrency crime cases.

Methodology

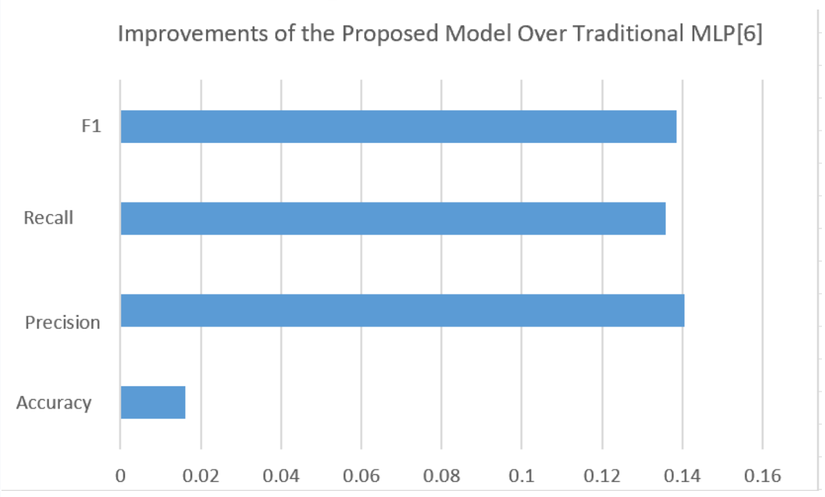


Experimental Settings

Dataset: Elliptic Bitcoin Dataset (4,545 illicit / 42,019 licit)
Data split: time-ordered, 34 train / 15 test snapshots (70/30)
Backbone: MLP (1 hidden layer, 100 units)
Training: 100 epochs, learning rate = 0.01
Framework: PyTorch
Metrics: Accuracy, Precision, Recall, F1-score

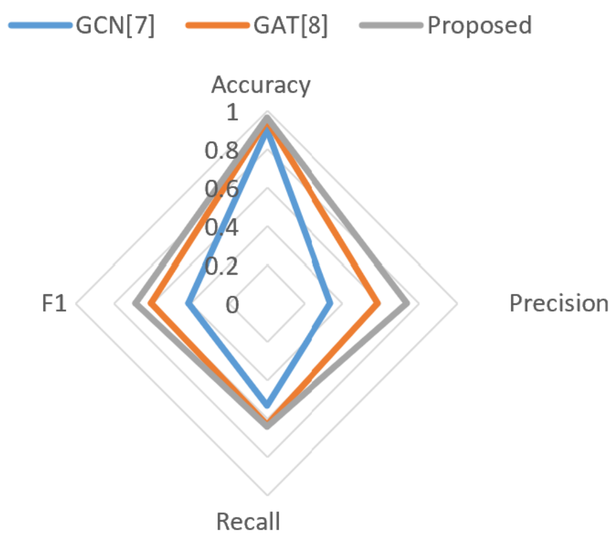
Experimental Results

1.Performance Comparison



2.Feature Combination Performance

3.Comparison with Mainstream Models



Conclusion

The proposed **multi-feature fusion** method, combining **LSTM**, **Random Walk**, and **PageRank** features, significantly enhances **illegal Bitcoin transaction detection**.

By incorporating **Focal Loss** to address **class imbalance**, the model demonstrates an exceptional ability to identify **illegal transactions** amidst the overwhelming majority of legal transactions.

Experimental validation shows that our method outperforms **traditional models** (MLP) and **graph-based models** (GCN, GAT), achieving the best overall performance in terms of accuracy, precision, recall, and F1 score.

Future Work

Further improvements can be made in **feature selection** and **model optimization** to enhance the detection accuracy in larger and more complex datasets.

The approach could be applied to other cryptocurrencies like **Ethereum** and **Tron**, expanding its applicability to **multi-cryptocurrency monitoring systems**.

Real-time monitoring systems can be developed using this approach to enable **proactive detection** of illicit transactions in Bitcoin and other digital currencies.

References

[1] Arnone G, Scire' G, Bivona E. The (mis) use of cryptocurrencies by criminal organizations: a systematic literature review[J]. Digital Finance, 2025: 1-37.
[2] HOCHREITER S, SCHMIDHUBER J. Long short-term memory [J]. Neural computation, 1997, 9(8): 1735-1780.
[3] LAWLER G F, LIMIC V. Random walk: a modern introduction [M]. Cambridge University Press, 2010.
[4] PAGE L, BRIN S, MOTWANI R, et al. The pagerank citation ranking: Bringing order to the web [J]. 1999.
[5] WEBER M, DOMENICONI G, CHEN J, et al. Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics [J]. arXiv preprint arXiv:1908.02591, 2019.
[6] Rosenblatt F. The perceptron: a probabilistic model for information storage and organization in the brain[J]. Psychological review, 1958, 65(6): 386.
[7] Kipf T N. Semi-supervised classification with graph convolutional networks[J]. arXiv preprint arXiv:1609.02907, 2016.
[8] Veličković P, Cucurull G, Casanova A, et al. Graph attention networks[J]. arXiv preprint arXiv:1710.10903, 2017.