Illegal Bitcoin Transaction Detection Using Pre-trained Language Models (BERT and Variants)

JIANG Xianbo, BAO Menghu, WANG Bo, XING Guidong , PENG Lei, YAN Shengdong, KANG Yanrong, CHU Chuanhong, GUO Lili, ZHAO Lu, ZHANG Qian, ZHANG Yaoguo,YANG Kunlin, NIE Leihang

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

Abstract

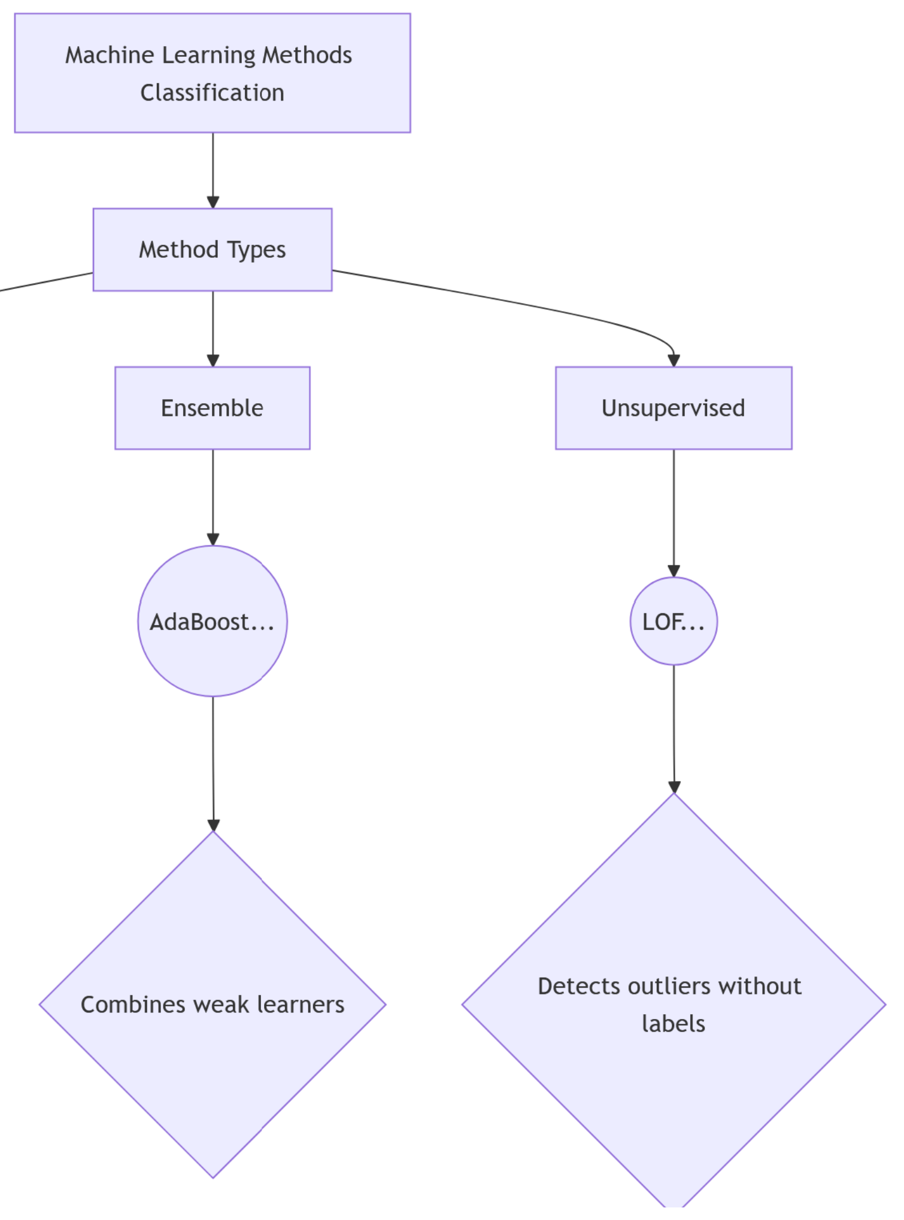
Bitcoin, the leading cryptocurrency since 2009, provides anonymity and decentralization, attracting illegal activities like money laundering and terrorism financing, which challenge global financial security and regulation. This study investigates the use of advanced natural language processing (NLP) models, specifically BERT and its variants (ModernBERT, RoBERTa, ALBERT, etc.), to detect illicit Bitcoin transactions. Using the BitcoinElliptic dataset, transaction features and relationships were converted into structured text data, and various BERT-based models were fine-tuned for classification.

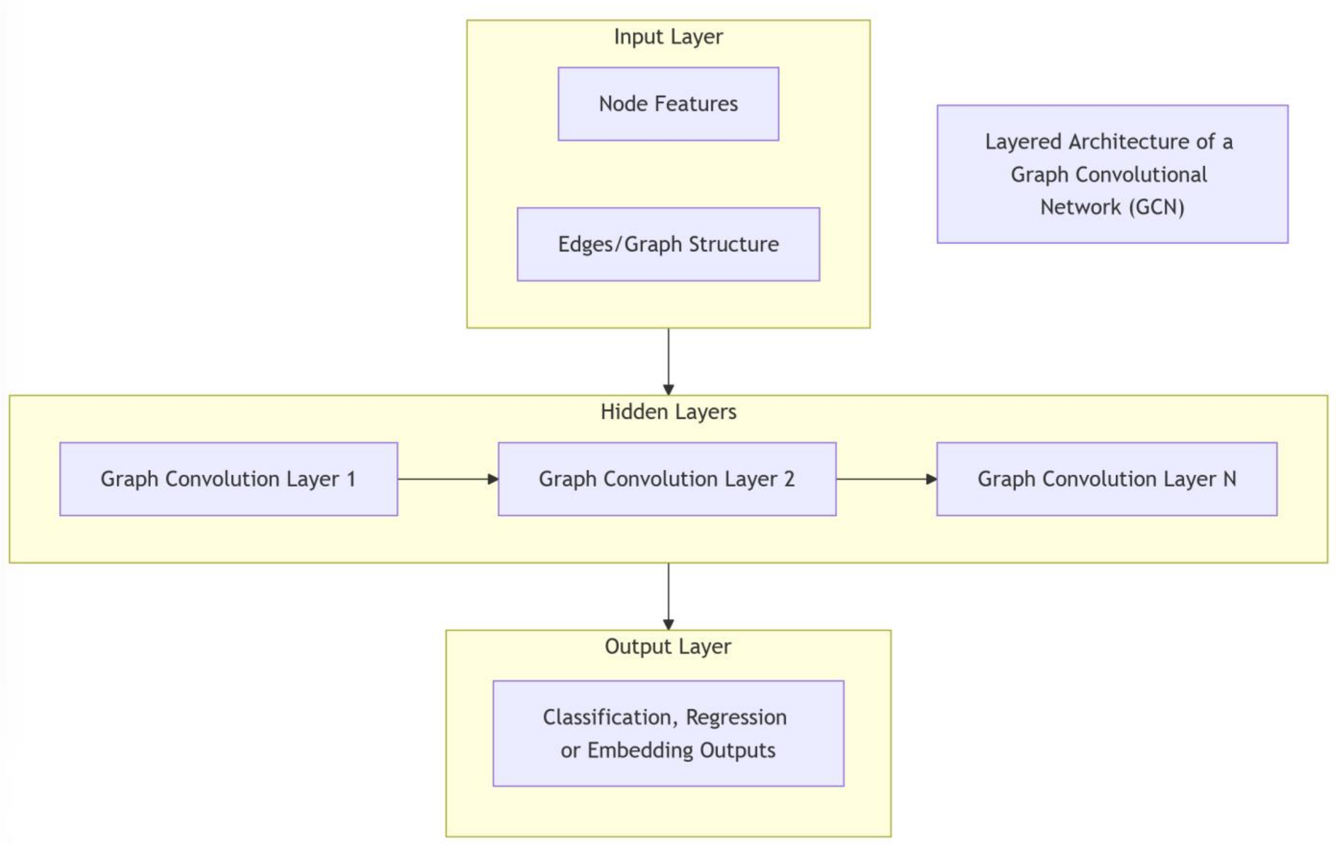
Related Work

Traditional Machine Learning Models: Algorithms like SVM, AdaBoost, and MLP detect illicit transactions using extracted features [1]. These methods face challenges with high-dimensional data and generalization

Deep Learning Models: CNNs and RNNs automatically extract features from large datasets [2], while GNNs analyze transaction networks to identify anomalies [3].

Pre-trained Language Models: BERT and its variants (e.g., RoBERTa, ALBERT) excel in NLP but are rarely applied to this domain.




Input Layer
Node Features
Edges/Graph Structure
Layered Architecture of a Graph Convolutional Network (GCN)
Hidden Layers
Graph Convolution Layer 1
Graph Convolution Layer 2
Graph Convolution Layer N
Output Layer
Classification, Regression or Embedding Outputs

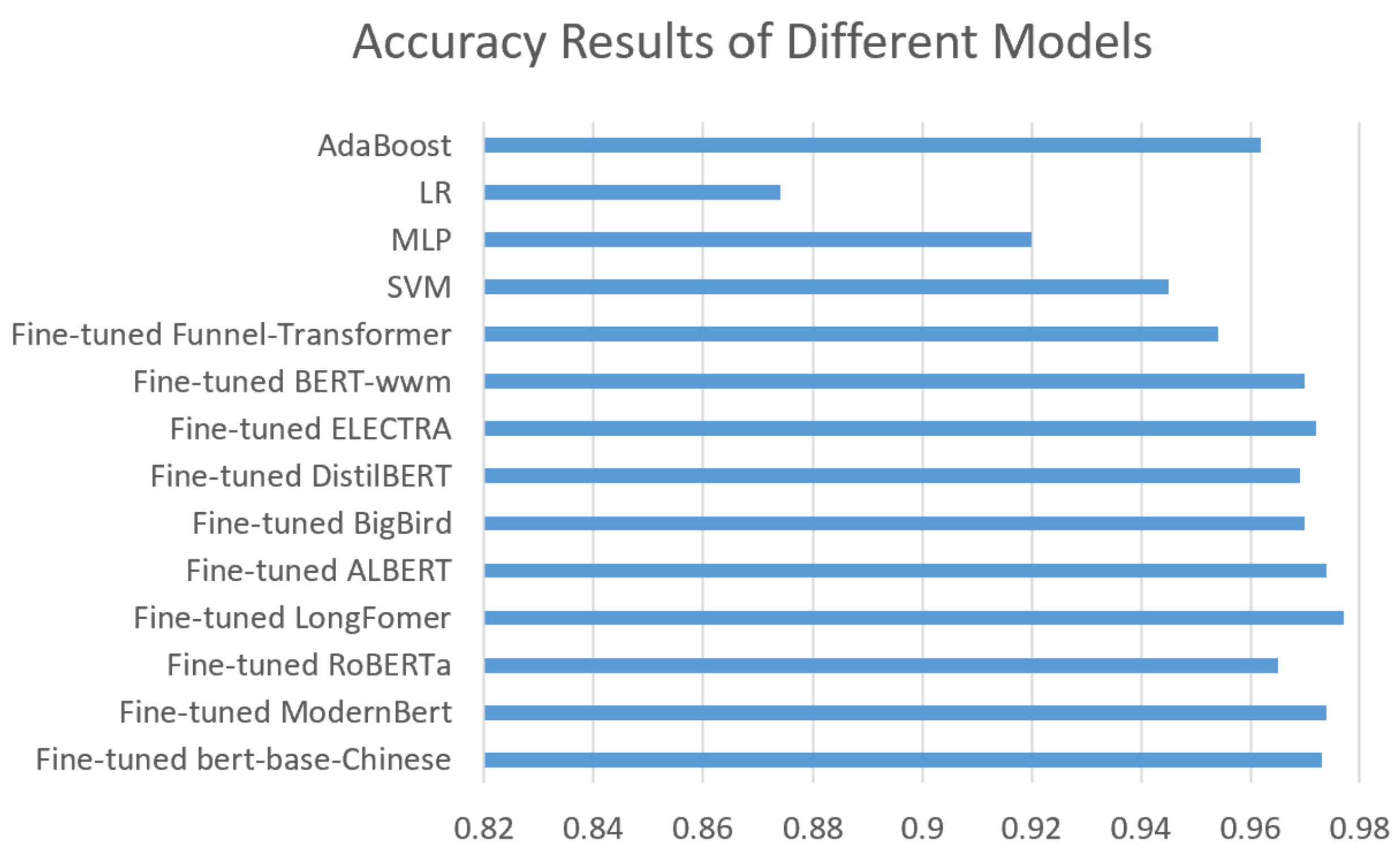
Experimental Setup:

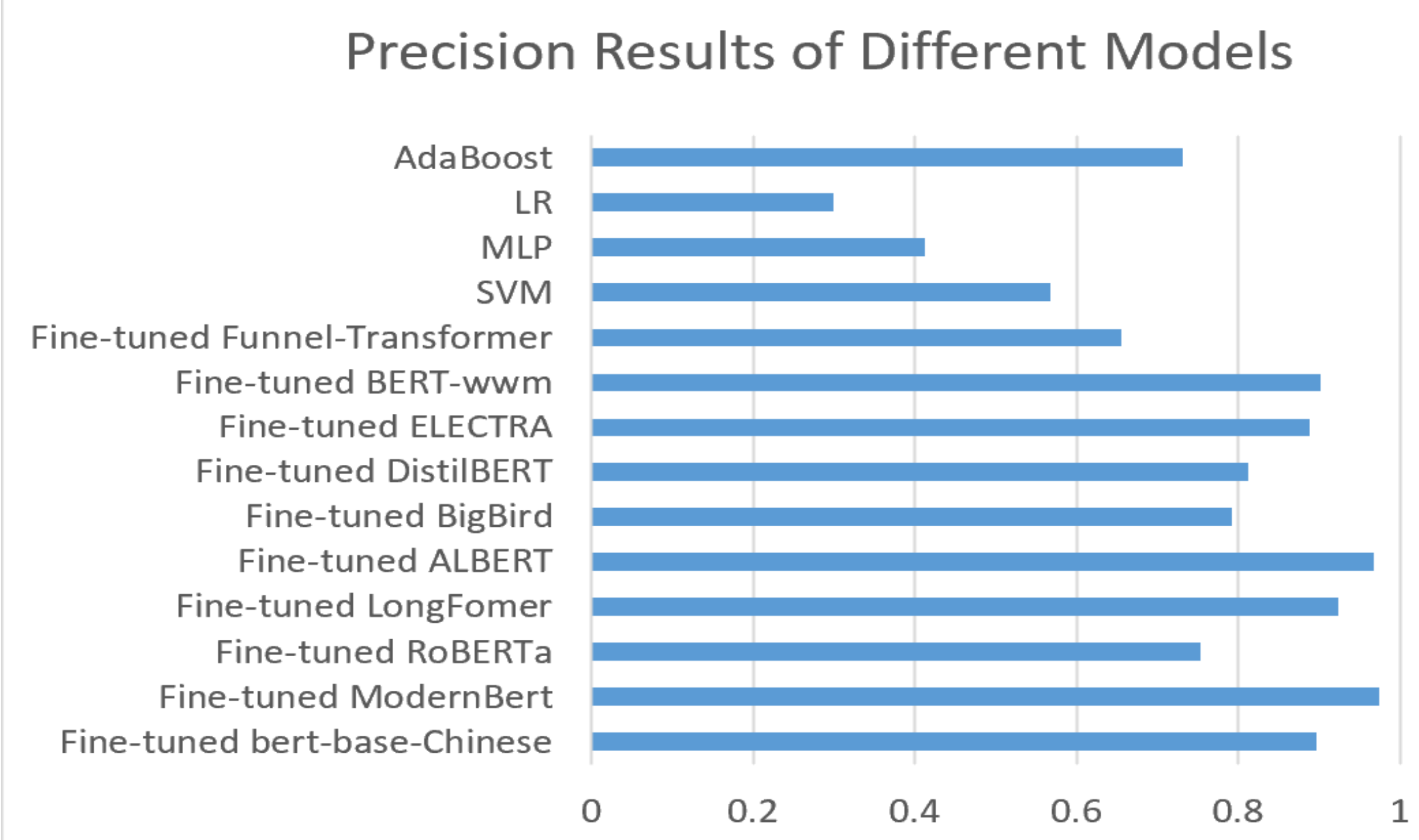
Dataset: BitcoinElliptic Dataset[4] includes 203,769 labeled transactions (legal and illegal) and 234,355 edges, split into 49 time segments. It is imbalanced, with 21% legal (42,019) and 2% illegal (4,545) transactions. We used 70% for training and 30% for testing.

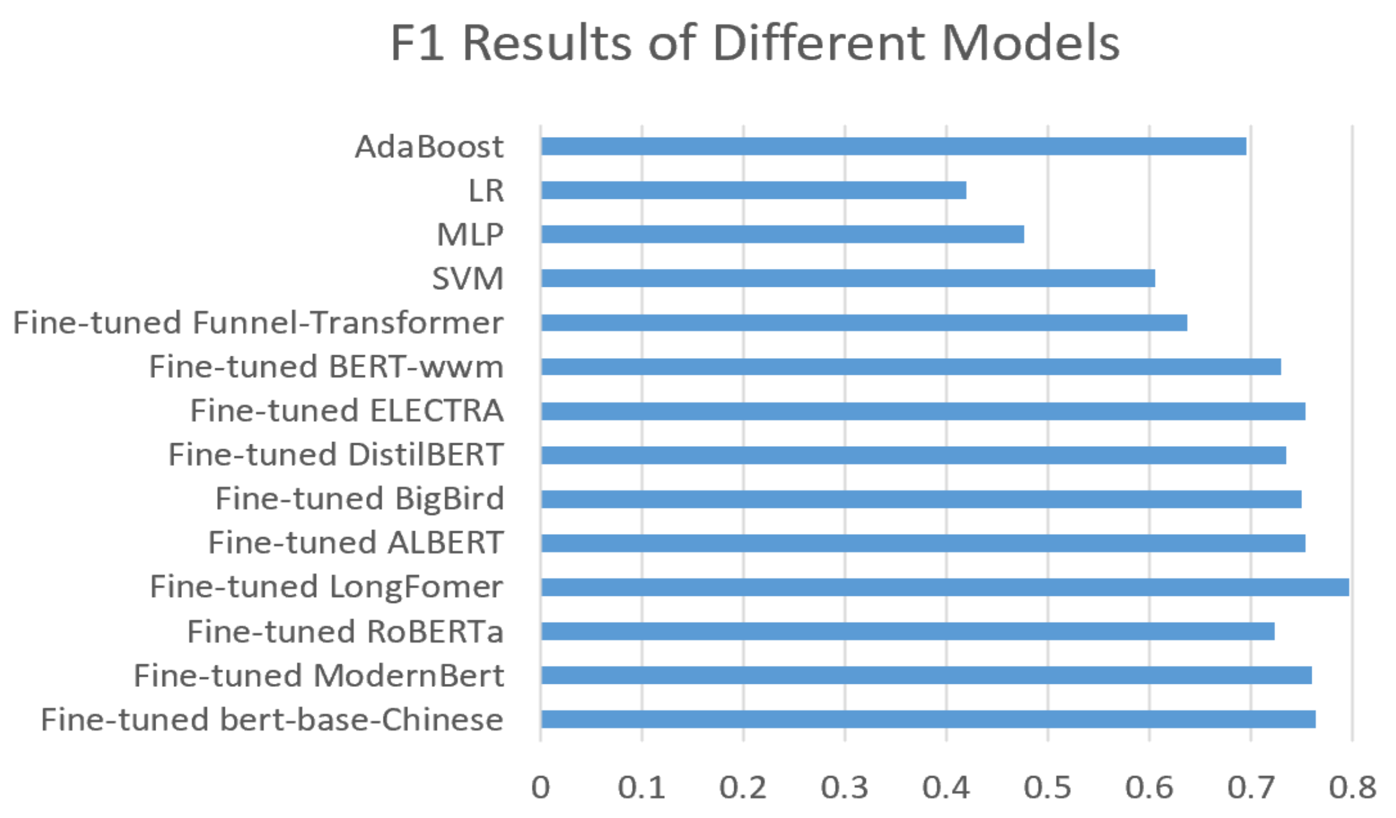
Model: Fine-tuned BERT variants (ModernBERT, RoBERTa, etc.) for classifying transactions as illegal or legal using Adam optimizer, 5e-5 learning rate, batch size 64, over 5 epochs.

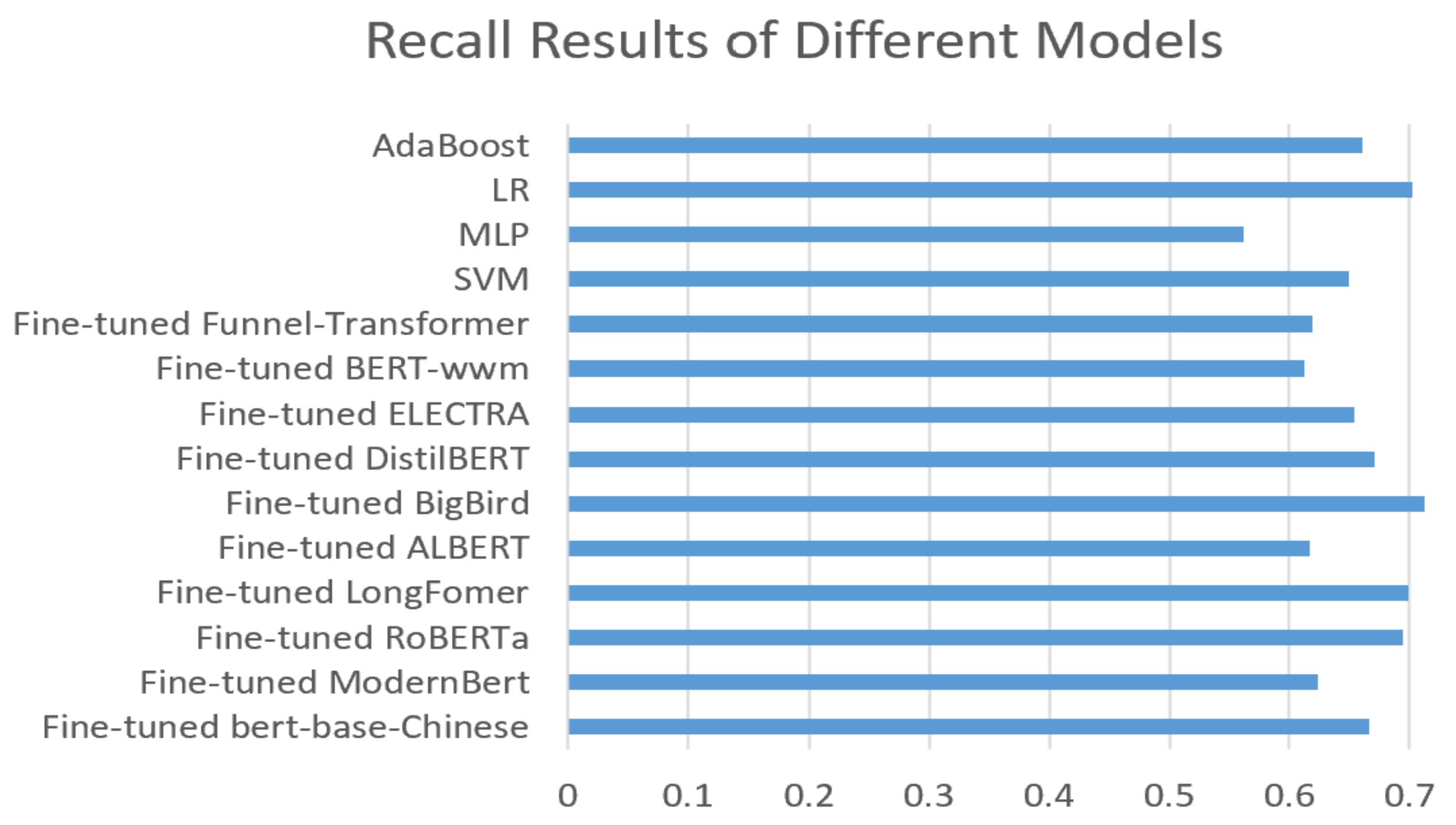
Setup: Intel Xeon CPU, 128GB RAM, NVIDIA RTX 4090 GPU; Windows 11, Python 3.9, PyTorch.

Experimental Results









Discussion

Strengths of BERT-based Models:

- **Superior Performance:** BERT-based models significantly outperform traditional models in accuracy, precision, and F1-score.
- **Complexity Handling:** These models handle complex, high-dimensional transaction data more effectively, capturing intricate patterns of illegal transactions.

Challenges:

- **Computational Cost:** BERT models require significant computational resources, which can be a limitation for real-time detection.
- **Data Quality & Variability:** The BitcoinElliptic dataset, while comprehensive, may not capture the full range of illegal Bitcoin activities. Future work will explore more dynamic and diverse datasets.

Future Work

Model Optimization: Research will focus on enhancing model efficiency, reducing training time, and optimizing the performance of large-scale models in real-time detection scenarios.
Exploring New Techniques: Combining BERT with other advanced techniques like Graph Neural Networks (GNNs) or Reinforcement Learning for continuous model adaptation as illegal trading methods evolve.
Dataset Expansion: Incorporating more diverse transaction data from different time periods and platforms to improve model generalization.

Conclusion

This study shows that fine-tuned BERT-based models enhance Bitcoin illegal transaction detection, supporting anti-money laundering (AML) and counter-terrorism financing (CTF) efforts. Future work will focus on optimizing these models and exploring new detection methods.

References

[1] CHEN B, WEI F, GU C. Bitcoin Theft Detection Based on Supervised Machine Learning Algorithms[J]. Security and Communication Networks, 2021, 2021: 1-10.

[2] Sun X, Yang T, Hu B. LSTM-TC: Bitcoin coin mixing detection method with a high recall[J]. Applied Intelligence, 2022, 52(1): 780-793.

[3] JIANG XIANBO, XING GUIDONG, KANG Yanrong, et al. A Bitcoin Illegal Transaction Detection Method Based on Graph Neural Networks [J/OL]. Forensic Science and Technology. https://doi.org/10.16467/j.1008-3650.2024.0052.

[4] WEBER M, DOMENICONI G, CHEN J, et al. Anti-money laundering in Bitcoin: experimenting with graph convolutional networks for financial forensics [J/OL]. arXiv preprint arXiv:1908.02591, 2019