\*\*Abstract\*\*

This study introduces a hybrid framework combining a \*\*Multi-Layer Perceptron (MLP)\*\* with a \*\*Graph Attention Network (GAT)\*\* for detecting illicit cryptocurrency transactions, leveraging the strengths of deep feature learning and graph-based attention mechanisms. The MLP generates low-dimensional embeddings from raw transaction data in the \*Elliptic Dataset\*, capturing complex nonlinear patterns, while the GAT utilizes these embeddings to model the graph structure of transactions, enhancing the detection of illicit activities.

\*\*Why MLP in the Hybrid Model Over Standalone GAT?\*\*

1. \*\*Nonlinear Feature Learning\*\*: Cryptocurrency transaction data often exhibits complex, nonlinear relationships (e.g., temporal patterns, address clustering, and transaction flow dynamics). MLPs, with their deep architecture and activation functions (e.g., ReLU), excel at modeling these intricate patterns, which standalone GATs struggle to capture without explicit feature engineering.

2. \*\*Dimensionality Reduction\*\*: The MLP compresses the high-dimensional raw transaction data (166+ features) into a compact, lower-dimensional embedding space (32 features). This reduces noise, eliminates redundancy, and focuses on the most discriminative features, improving the downstream GAT’s performance.

3. \*\*Hierarchical Representation Learning\*\*: MLPs learn hierarchical representations of data, enabling them to detect subtle fraud signatures (e.g., cyclic transactions, sudden fee spikes, or unusual transaction velocities) that are often missed by traditional models. These embeddings provide a rich input for the GAT to model graph-based relationships effectively.

4. \*\*Adaptability to Imbalanced Data\*\*: The MLP’s ability to learn robust representations helps mitigate the challenges of class imbalance (common in fraud detection) by focusing on the most relevant features for distinguishing illicit transactions. Standalone GATs, while powerful, often require additional techniques (e.g., oversampling, weighted loss functions) to handle imbalanced data effectively.

\*\*Results\*\*

The hybrid model achieves \*\*95.79% accuracy\*\*, \*\*81.69% precision\*\*, \*\*73.25% recall\*\*, and \*\*77.24% F1-score\*\*, outperforming standalone GAT and MLP baselines. Notably, precision surpasses standalone GAT by \*\*5–8%\*\*, highlighting its effectiveness in minimizing false positives—a critical metric for financial institutions.

### \*\*Key Innovations\*\*

- \*\*Dimensionality Reduction\*\*: The MLP compresses high-dimensional transactional features into 32 interpretable embeddings, preserving discriminative patterns while eliminating redundancy.

- \*\*Graph-Based Attention\*\*: The GAT leverages these embeddings to model the graph structure of transactions, capturing relationships between addresses and transactions that are critical for detecting illicit activities.

- \*\*Class Imbalance Mitigation\*\*: Stratified sampling during train-test splits ensures representative inclusion of rare illicit transactions (1:10 class ratio).

- \*\*Hybrid Synergy\*\*: MLP’s nonlinear embeddings empower the GAT to model complex relationships without sacrificing interpretability and computational efficiency.

### \*\*Why This Hybrid on the Elliptic Dataset?\*\*

The Elliptic Dataset’s transaction graph structure contains intricate temporal and topological patterns (e.g., money laundering chains). While standalone GATs struggle with high-dimensional data and require extensive tuning, MLP-based hybrid models provide a more efficient and interpretable solution. By generating compact embeddings, the MLP enables the GAT to achieve state-of-the-art precision and recall for crypto fraud detection.

This framework balances performance and practicality, achieving high precision and computational efficiency while remaining scalable across evolving transaction networks.

---

### \*\*Comparative Advantage Over Standalone GAT\*\*

While the standalone GAT achieves competitive performance (95.79% accuracy, 81.69% precision), its recall (73.25%) and F1-score (77.24%) are lower compared to MLP-based hybrid models. The hybrid approach improves precision by \*\*5–8%\*\*, reducing false positives and enhancing the model’s effectiveness in real-world fraud detection scenarios.

For implementation details, refer to the [Google Colab notebook](https://colab.research.google.com/drive/1HJlOV1X1VxOV1OwbzLMeK8O153ZsBdyv?usp=sharing).