FraudLens: Graph Structural Learning for Bitcoin Illicit Activity Identification

Jack Nicholls, Dr. Aditya Kuppa, Assoc. Prof. Dr. Nhien-An Le-Khac

University College Dublin
School of Computer Science,
Ireland
• Crypto in the news:
  • June 2022: Binance enabled $2.35 billion in laundering.
  • 2023: $500m in ransomware payments.
  • Tornado cash: $1 billion laundered crypto.

• Increasing regulation on transparency and trading.

• Research focuses on GNN variations and enhancements rather than preprocessing and topology imbalance.

Crypto crime hits record $20 bln in 2022
Contributions

• Identify label and topology imbalance issues impacting GNN models in identifying illicit activity in bitcoin.

• Propose two novel model-agnostic methods for graph structure learning that address the imbalances and discover fraudulent nodes in bitcoin transaction graphs.

• Evaluate methods on a highly imbalanced and temporal Elliptic Bitcoin dataset to show performance improvement.

• Compare methods against other imbalanced node classification techniques on DBLP citation network to show effectiveness.
Cryptocurrency

- Computational method of transferring digital value between users.
- Does not require financial intermediary.
- Introduced blockchain technology.
- Two main models of development:
  - UTxO.
  - Account-based.
- Basis for digital currency.
Decentralised
Blockchain
Digital Asset
Programmable

**Traditional Account-Based Transactions**

Alice → Bob
€500

**UTxO Bitcoin Transaction**

Alice → Bob
0.75BTC

A (Alice) 1BTC

B₁ (Bob) 0.75

Aₐ (Alice) 0.25

**UTxO**: Unique method of transferring value without a financial intermediary.

An output represents Bitcoin that can be spent by a user who has the private key.
Bitcoin and Illicit Activity

Money Laundering

Dark Market Purchases

Terrorist Financing

Organized Crime Financing

State bodies cybercrime
How to launder?

Mixing
Obfuscates origin of user’s Bitcoin by blending them with many others.

CoinJoin
Multisignature transaction made available through privacy wallets and services.

Input $A$
Input $B$
Input $C$

CoinJoin Tx:
3 Senders
3 Receivers

Output $A$
Output $B$
Output $C$

Mixed funds deposited to new wallet
Heuristics

Denonymise the Bitcoin network

Group inputs into clusters

Heavy assumptions

Broken
Heuristics

Multi-Input/Co-Spend
Clusters the inputs in a transaction and links them to a controlling entity
Heuristics

**Multi-Input/Co-Spend**
Clusters the inputs in a transaction and links them to a controlling entity.

**Change Address**
Classifies one of the outputs as change in a standard transaction.
Heuristics

Multi-Input/Co-Spend
Clusters the inputs in a transaction and links them to a controlling entity

Change Address
Classifies one of the outputs as change in a standard transaction

Smallest amount must be change in transaction.
Deep Learning in Illicit Activity Identification

Heuristics have high avg. error rate (63.46% for co-spend, 92.66% for change address)\(^1\).

Complementing heuristics with ML\(^2,3\).

Graph Neural Networks show promise in classification and deanonymisation tasks\(^4,5\).

Bitcoin is naturally a graph.
Bitcoin Graph – Transaction Level

Classic Edges – Transaction flow

Timestep 1

Normal Tx: 1 Input 1 Output

Normal Tx: 1 Input 2 Outputs

Timestep 2

Normal Tx: 1 Input 1 Output

Timestep 3

Normal Tx: 1 Input 1 Output

Timestep 4

Normal Tx: 2 Input 1 Output
Illicit/Licit Labels

- How do we capture the relationship between illicit nodes?
- Can we restructure the graph based on underlying properties and similarity between nodes?
- Does this improve model’s performance?
Bitcoin Graph Topology

• Topology imbalance in Bitcoin is a major issue in illicit activity detection.

• Three key aspects of graph class-imbalance are unique against classical class-imbalanced tasks in ML.
  1. Graph data is unique and non-Euclidean. Traditional methods may struggle to handle complex connectivity patterns in graph data.
  2. Mishandling the graph relationships through under and oversampling can disrupt the rich relational information.
  3. Specialized techniques are needed to preserve and leverage the information.
Edges based on Affinity (EA)

Edges created based on node connectivity through Personalised Page Rank (PPR). Edge is created if connectivity score reaches parameter threshold.

Measure connectivity influence of illicit nodes using PPR.

Establish new edges if connectivity over threshold.
To restructure a graph using EA:

- Using temporal graph, $G$, and create subgraph, $G_L$, with labelled illicit nodes ($V_L$).

- Pick random nodes, $u_i$ and $V_L$, from $G$ and $G_L$ respectively.

- Apply function beta (PPR) to measure connectivity influence between $V_L$ and $u_i$.

- Select all nodes, $u_i$, with the highest affinity to $V_L$ and select all the edges between them to create new adjacency matrix $A^*$. 

---

**Algorithm 1** Edges based on Affinity (EA) Method

**Require:** Original graph $G$ per temporal step, $G'_t$ graph containing only labeled illicit nodes at training time and target ratio $p \in (0, 1)$.  

1. $n, n' \leftarrow$ Pick random nodes from $G$ and $G'_t$, respectively  
2. for $(G_t, n_t) \in \{(G, n), (G'_t, n')\}$ do  
3. $s_t \leftarrow$ Calculate connectivity scores of nodes $\beta(G_t, n_t)$  
4. $S_t \leftarrow$ Select $k$ nodes having the largest scores in $s_t$  
5. $S \leftarrow S_t$ if $G_t = G$ otherwise $S' \leftarrow S_t$  
6. end for
Edges based on Node Features (ENF)

Edges created based on node feature similarity. MLP calculates embeddings and sigmoid function used to find probabilistic cut-off.

Original Graph

Restructured Graph

Node features similarity is compared using MLP.

A sigmoid function is used to decide whether an edge is created or not.

Low similarity scores are considered noisy and removed.
Edges based on Node Features (ENF)

• For each temporal graph, G, calculate embeddings, Z, for each node, u, against random node, v.

\[ Z(u) = \theta(X(u)) \]

\[ \pi_{u,v} = \text{sigmoid} \left( Z(u)Z(v)^T \right) \]

Where \( \theta \) is a two-layer perception network, \( \pi_{u,v} \) denotes the strength of similarity between node u and v.

• Create probability of forming edges using learning attention weights \( \pi_{u,v} \) in a parameterized matrix \( P_{uv} = \{\pi_{u,v}\} \)

\[ p_{uv} = \frac{\exp(\pi_{uv})}{\sum_u \exp(\pi_{uv})} \]
Pipeline

1. Experimental Graph Dataset
2. Node Feature Enhancement, Scaling and Normalisation
3. Dataset Train/Test Split
4. Train Graph Dataset
5. Test Graph Dataset
6. GNN Evaluation
7. Graph Restructure Method (EA, ENF)
8. Deploy
9. Rolling Window Transaction Data
Graph Neural Networks (GNNs)

- Relationship between data points (edges)
- Requires nodes, edges, and node features.
- Different architectures focus on different aggregation methods.
- Creates embeddings representative of nodes and their neighbourhood.

<table>
<thead>
<tr>
<th>GNN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graph Convolutional Network (GCN)(^6)</td>
</tr>
<tr>
<td>Graph Attention Transformer (GAT)(^7)</td>
</tr>
<tr>
<td>GraphSAGE(^8)</td>
</tr>
<tr>
<td>Generalised PageRank (GPRGNN)(^9)</td>
</tr>
<tr>
<td>Explore-to-Extrapolate Risk Minimization (EERM)(^{10})</td>
</tr>
</tbody>
</table>
H: Can we improve GNN performance of an imbalanced node classification task using proposed EA and ENF methods?

1. **Elliptic Bitcoin temporal graph dataset:**
   - Train 5 GNNs using new structured graphs from EA and ENF.
   - Compare against baseline random forest.

2. **Compare node imbalance techniques** against proposed EA and ENF methods on DBLP citation network.
   - Demonstrate model agnostic and multi-domain applicability of methods.
Bitcoin Dataset

- Largest labelled dataset for cryptocurrency illicit activity.
  - 203,769 nodes
  - 49 time-steps
  - 166 features
  - 21% labelled licit
  - 2% labelled illicit

- Labelled through heuristics-based reasoning.

- Popularly researched.

- We train on the first 7-11 timesteps

- We test on time steps 34-49 timesteps.

- Elliptic++ (2023)
Results – Elliptic Dataset

F1-score is metric of evaluation.

\( G^{EA} \) = Graph created from EA  
\( G^{ENF} \) = Graph created from EA  
\( G \) = Original Graph

Even in highly imbalanced temporal steps 43–49, GNNs identify illicit transactions.

ENF shown to be the most impactful method of graph restructuring.

<table>
<thead>
<tr>
<th>Graph</th>
<th>GNN-Arch/Model</th>
<th>Timestep 34-38</th>
<th>Timestep 39-42</th>
<th>Timestep 43-46</th>
<th>Timestep 47-49</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>RF</td>
<td>85.49</td>
<td>78.67</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>( G^{EA} )</td>
<td>GCN</td>
<td>51.33</td>
<td><strong>52.33</strong></td>
<td>49.16</td>
<td>44.07</td>
</tr>
<tr>
<td>( G^{ENF} )</td>
<td></td>
<td>47.59</td>
<td>48.38</td>
<td><strong>49.62</strong></td>
<td>46.61</td>
</tr>
<tr>
<td>( G )</td>
<td></td>
<td>48.86</td>
<td>47.79</td>
<td>48.69</td>
<td><strong>46.65</strong></td>
</tr>
<tr>
<td>( G^{EA} )</td>
<td>GAT</td>
<td>56.75</td>
<td>53.76</td>
<td>48.16</td>
<td>46.432</td>
</tr>
<tr>
<td>( G^{ENF} )</td>
<td></td>
<td><strong>68.58</strong></td>
<td><strong>58.19</strong></td>
<td>47.32</td>
<td><strong>52.97</strong></td>
</tr>
<tr>
<td>( G )</td>
<td></td>
<td>50.39</td>
<td>50.26</td>
<td><strong>49.01</strong></td>
<td>46.80</td>
</tr>
<tr>
<td>( G^{EA} )</td>
<td>Graph-SAGE</td>
<td>61.54</td>
<td>59.25</td>
<td><strong>54.15</strong></td>
<td>46.55</td>
</tr>
<tr>
<td>( G^{ENF} )</td>
<td></td>
<td><strong>65.86</strong></td>
<td><strong>62.73</strong></td>
<td>49.58</td>
<td><strong>46.97</strong></td>
</tr>
<tr>
<td>( G )</td>
<td></td>
<td>56.06</td>
<td>50.23</td>
<td>49.39</td>
<td>46.41</td>
</tr>
<tr>
<td>( G^{EA} )</td>
<td>GPR-GNN</td>
<td>67.92</td>
<td>63.44</td>
<td>48.22</td>
<td>44.02</td>
</tr>
<tr>
<td>( G^{ENF} )</td>
<td></td>
<td><strong>72.73</strong></td>
<td>61.37</td>
<td><strong>49.73</strong></td>
<td><strong>46.69</strong></td>
</tr>
<tr>
<td>( G )</td>
<td></td>
<td>67.34</td>
<td><strong>67.25</strong></td>
<td>47.91</td>
<td>44.34</td>
</tr>
<tr>
<td>( G^{EA} )</td>
<td>EERM</td>
<td>76.05</td>
<td>78.09</td>
<td>62.65</td>
<td>49.91</td>
</tr>
<tr>
<td>( G^{ENF} )</td>
<td></td>
<td><strong>76.35</strong></td>
<td><strong>78.34</strong></td>
<td><strong>63.92</strong></td>
<td><strong>50.45</strong></td>
</tr>
<tr>
<td>( G )</td>
<td></td>
<td>73.05</td>
<td>75.33</td>
<td>59.45</td>
<td>49.42</td>
</tr>
</tbody>
</table>
ENF and EA method tested with GAT.

**ENF** consistently **outperforms** against other node imbalance classification techniques.
Discussion

• GNN models can identify illicit transactions well in each timestep segment even with heavy class imbalance.

• Edge Affinity (EA) and Edge Node Features (ENF) consistently outperform original graph.

• EA and ENF are model and domain agnostic.

• Preprocessing of MLOps Pipeline.

• Potential for identifying mixing and CoinJoin operations.

• Wider applicability in financial cybercrime activity detection
Future Work & Limitations

• Improving performance and testing on more datasets.

• Rich node features required to gauge similarity.

• Integrating LLM to interpret transactions and create narratives for investigation.
Thank You

Jack Nicholls
Email: jack.nicholls@ucdconnect.ie

Dr. Aditya Kuppa
Email: aditya.kuppa@ucd.ie

Assoc Prof. An Le
Email: an.lekhac@ucd.ie

LinkedIn: https://www.linkedin.com/in/jack-nicholls93/

Twitter/X: https://twitter.com/JackPNicholls
Sources