Jennifer Payne
s3932835@student.rmit.edu.au

Introduction

Anti-money laundering (AML) and transaction monitoring on the blockchain is an emerging area that has gained attention and significance as cryptocurrency moves into the mainstream. The chosen topic of research is 'Money Laundering Networks on the Blockchain from Illicit Accounts' under the supervision of Dr Son Hoang Dau. This research aims to contribute to Anti-Money Laundering Counter Terrorism Financing (AML/CTF) programs by identifying money laundering networks on the blockchain, outside of a traditional banking system.

While AML detection models are extensively used in industry to counter financial crime, most focus on binary classification of suspicious actors or accounts[1][2]. However, criminal activity is often undertaken by large syndicates than lone wolves. This means that effective detection of money laundering networks needs to aim to identify multiple actors within the same network, rather than individuals in silos. This gap has created a research opportunity to explore ways to enhance existing binary classification algorithms using network analysis to capture multiple actors within a transaction path. The successful detection of a criminal network gives hope to moving one step closer to stopping the crime all together.

Money laundering is a criminal process of taking illicit funds made from predicate offences - such as human trafficking, drug trafficking or fraud - and cleaning the funds to appear legitimate[3]. After the criminal has acquired the funds, then the money laundering process begins to hide the true origins of the funds and distance the end beneficiary from the origin as much as possible[3]. This money laundering process includes 3 key stages: placement into a financial system, layering of funds through different financial institutions, jurisdictions, trusts and stores of value and finally integration of the cleaned funds back into the financial system to use without detection[3]. Successful laundering money confirms large profits can be made from illegal activities that result in a high negative impact on the most vulnerable members of society. Once cleaned, these funds can be used purchase large ticket items such as real estate, fund lavish lifestyles or reinvest in criminal activities. There is an estimated $10b to $15b AUD of money laundered in Australia every year from organised crime through sophisticated processes[3].

Cryptocurrency has become an increasingly popular medium to launder money due to the psuedo-anonymous nature of the blockchain, limited cross-border controls and speed of transfer. Once illicit funds are converted from fiat currency to cryptocurrency, money can be laundered by different layering techniques such as transferring illicit funds through multiple digital wallets, mixing services, and converting them into various cryptocurrencies to obscure the origin and destination[4]. Cryptocurrency is still used launder money despite falling under regulation like the US Bank Secrecy Act requiring requiring domestic and foreign money service businesses and financial institutions to report transactions over $10,000 USD[4].

The motivation of this paper to detect criminal syndicates or networks of people involved in a criminal syndicate by following the money through the blockchain. For simplicity, the focus of this research topic is on money laundering of illicit funds through the Bitcoin network.

1 Literature Review

Existing literature covers the current state of money laundering detection both in fiat currencies and cryptocurrencies. While the currency or jurisdiction may vary, as there are similarities in the money laundering process by criminal syndicates, the lessons and methodologies are universal.

1.1 Anti-Money Laundering in Fiat Currencies

Many jurisdictions require financial institutions and money service businesses by law to have an Anti-Money Laundering Counter Terrorist Financing (AML/CTF) program to prevent and report financial crime. In Australia, the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 [5] [6] dictates the minimum

legal requirements reporting entities need to comply with the AML/CTF regulation. This includes having a transaction monitoring system [2], Know-Your-Customer and ongoing customer due diligence checks, customer monitoring lists (e.g. for Politically Exposed Persons or PEPs), and submit Suspicious Matter Reports to Australian Transaction Reports and Analysis Centre (AUSTRAC), the Australian AML/CTF regulator [5].

Detecting financial crime is as much a balance between proactively screening for criminal behaviour to prevent financial crimes as it is meeting minimum regulatory requirements to avoid fines. For this reason, banks' transaction monitoring systems often use traditional rule- and scenario-based approaches (e.g. if-else statements) to detect suspicious transactions making the fight against money laundering a slow and ongoing challenge of balancing risk management and compliance [1]. Traditional AML programs are labour-intensive, resource-heavy processes given teams of analysts and investigators required to manually maintain the models and investigate the output. These processes are manually maintained and struggle to keep up with the sophisticated and evolving tactics of money launderers. Once an alert is created from a threshold-based model, the investigative process follows the below steps in Figure 1.

Recently, there has been a shift towards using machine learning to replace threshold rule-based models, including the use of binary classification [7] and network analysis[1].

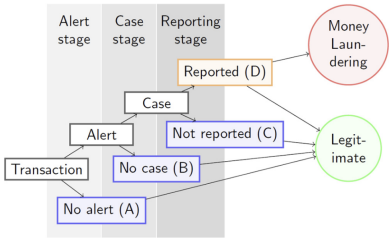

Figure 1: Banking Investigation Process Following Alert [7]

1.2 Anti-Money Laundering in Cryptocurrencies

Cryptocurrency exchanges are required to adhere to the same anti-money laundering (AML) regulations as financial institutions and money service businesses to prevent illicit activities. In the United States, the Bank Secrecy Act (BSA) mandates that cryptocurrency exchanges implement AML programs, verify user identities (KYC), monitor transactions, and report suspicious activities to the Financial Crimes Enforcement Network (FinCEN)[4][8]. Exchanges based in or operating within the US must register with FinCEN and comply with these regulations. Similarly, in Australia, the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 requires exchanges to register with AUSTRAC, conduct KYC procedures, report suspicious transactions, and maintain transaction records[5].

Despite these regulations, money laundering using cryptocurrencies still exists, particularly through exchanges that do not enforce KYC checks[9]. These non-compliant exchanges are often based in jurisdictions with lax or non-existent AML regulations, making it easier for illicit activities to go undetected. This regulatory gap highlights the ongoing challenge in the global fight against financial crime in the cryptocurrency space.

1.3 Binary Classification for AML Detection on Blockchain

The interest and application of AML models to detect financial crime on the blockchain has increased as labelled transaction datasets have become publicly available. Binary classification algorithms such as Logistic Regression, Random Forest, and Multilayer Perceptrons provide a clear and methodical approach to detecting illicit transactions within blockchain data and a benchmark in AML detection.

There are two key publicly-available datasets containing labelled Bitcoin transactions and actors as illicit, licit or unknown, called the Elliptic [10][11] and Elliptic++ datasets [12][13]. The Elliptic dataset was released in 2019 containing 203k directional Bitcoin transaction pairings, transaction features and classes identifying it as licit, illicit or unknown based on heuristic reasoning [10]. The Elliptic++ dataset, released in 2023, builds on the Elliptic dataset by adding wallet information and labels the actors of the transactions as licit, illicit or unknown.

Supervised machine learning techniques to classify transactions or actors as illicit or licit has been applied to these datasets with varying results. In Weber et al (2019), Logistic Regression, Random Forest and Graph Convolutional Networks were used on local and aggregated features from the nearest neighbours (one hop forwards/backwards) to classify transactions into illicit or licit categories. The recall (number of correctly predicted illicit transactions out of actual illicit transactions) varied between 0.5 and 0.7, with recall improving with the inclusion of neighbouring features, as seen in Figure 2. Random Forest with neighbouring node embeddings had the best performance across precision, recall and F1 compared to other classification models.

Binary classification is also applied to the Elliptic++ dataset to classify actors as illicit or licit, with Random Forest outperforming other models with a recall of 0.789 as in Figure 3. Random Forest is well-suited for handling imbalanced transaction datasets in fraud detection compared to Logistic Regression and Neural Networks, as we see in the model performance in Figure 2 and Figure 3. This is due to its ensemble approach, which combines multiple decision trees to enhance its ability to manage class imbalance effectively. By using techniques like bootstrap sampling and random feature selection, Random Forest focuses on misclassified instances, improving detection of rare fraudulent transactions. Additionally, it captures complex interactions between features with minimal preprocessing and is less prone to overfitting, making it a robust choice for identifying fraud within a large volume of legitimate transactions[14].

Table 1: Illicit classification results. Top part of the table shows results without the leverage of the graph information, for each model are shown results with different input: *AF* refers to all features, *LF* refers to the local features, i.e. the first 94, and *NE* refers to the node embeddings computed by GCN. Bottom part of the table shows results with GCN.

Method	Illicit			MicroAVG
	Precision	Recall	F_1	F_1
Logistic Regr^{AF}	0.404	0.593	0.481	0.931
Logistic Regr^{AF+NE}	0.537	0.528	0.533	0.945
Logistic Regr^{LF}	0.348	0.668	0.457	0.920
Logistic Regr^{LF+NE}	0.518	0.571	0.543	0.945
RandomForest^{AF}	0.956	0.670	0.788	0.977
RandomForest^{AF+NE}	0.971	0.675	0.796	0.978
RandomForest^{LF}	0.803	0.611	0.694	0.966
RandomForest^{LF+NE}	0.878	0.668	0.759	0.973
MLP^{AF}	0.694	0.617	0.653	0.962
MLP^{AF+NE}	0.780	0.617	0.689	0.967
MLP^{LF}	0.637	0.662	0.649	0.958
MLP^{LF+NE}	0.6819	0.5782	0.6258	0.986
GCN	0.812	0.512	0.628	0.961
Skip-GCN	0.812	0.623	0.705	0.966

Figure 2: Elliptic Binary Classification of Transactions Results[10]

However, there are limitations with binary classification for anomaly detection as the approach focuses on the detection of individual nodes in silos, rather than multiple individuals that are part of the same transaction network. Figure 4 is an example of how binary classification may detect illicit actors individually, but fails to detect a mutliple actors within the same criminal network. This fictitious example was built using python package 'networkx' [15] and shows a money laundering network with multiple money mules. Charlie, the red node, is detected in a transaction monitoring system which uses binary classification, investigated and arrested. The criminal syndicate then replaces Charlie with Ben (the grey node) and the money laundering cycle continues.

Table 9: Illicit actors results using individual/ensemble of classifiers. AR is classification on our Elliptic++ actors dataset.

Model	Precision	Recall	F1 Score	Micro-F1
LR^{AR}	0.477	0.046	0.083	0.964
RF^{AR}	**0.911**	**0.789**	**0.845**	**0.990**
MLP^{AR}	0.708	0.502	0.587	0.974
LSTM^{AR}	0.922	0.033	0.064	0.965
XGB^{AR}	0.869	0.534	0.662	0.980
2 ***classifiers ensemble***, *selecting top* 3 *classifiers*				
RF+MLP^{AR}	0.967	0.403	0.568	0.978
RF+XGB^{AR}	**0.959**	**0.530**	**0.682**	**0.982**
MLP+XGB^{AR}	0.929	0.324	0.481	0.975
3 ***classifiers ensemble***, *selecting top* 3 *classifiers*				
RF+MLP+XGB^{AR}	**0.933**	**0.572**	**0.709**	**0.983**

Figure 3: Elliptic++ Binary Classification of Actors Results[12]

This limitation has become evident as both research and AML programs are shifting towards the use of network analysis to detect criminal syndicates.

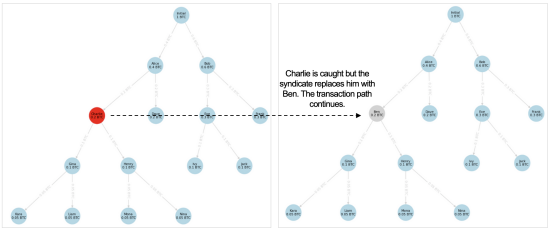

Figure 4: Example of a Money Laundering Network with Money Mule Replacement

1.4 Network Analysis for AML Detection on Blockchain

Network analysis has emerged as a powerful tool for AML detection in Bitcoin transactions, addressing the limitations of traditional binary classification methods that detect actors in isolation rather than considering their interconnected activities within the transaction network. By leveraging graph-based algorithms, network analysis can uncover complex patterns and relationships among multiple actors involved in money laundering schemes, such as enhancing independent features with n-hop neighbouring information, analysing the cluster density or the depth of networks.

An effective technique is the application of Google's PageRank algorithm[16] to a transaction path or subnetwork. Originally designed to rank web pages based on their link structure, PageRank can be applied to transaction information by assigning a score to each node (representing a wallet or account) that reflects its relative importance or influence within the network[17]. In the context of AML, this score can help identify key actors involved in money laundering by evaluating the flow and frequency of transactions between nodes[18].

The PageRank algorithm works by simulating a random walk through the transaction graph, where the probability of moving from one node to another is determined by the number of outgoing transactions from each node. Nodes that receive more transactions from other influential nodes (those with high PageRank scores) are themselves assigned higher scores. This iterative process continues until the PageRank scores converge, providing a stable ranking of nodes based on their transaction behaviour[16]. Figure 5 shows how PageRank can be applied to a fictitious money laundering transaction path.

Applying PageRank to AML detection offers several advantages. First, it considers the entire transaction network rather than isolated nodes, allowing for the identification of complex money laundering layering techniques where multiple actors are involved. This holistic approach helps to detect complex laundering activities that might go unnoticed with simpler classification methods at a transaction or actor level. Second, by focusing on the connectivity and influence of nodes, PageRank can highlight not only the most active nodes but also those that play a critical role in the flow of illicit funds. As the PageRank algorithm places higher importance to nodes that have more inbound links connected to it, this algorithm can be applied to transaction paths to identify more important or key persons in a criminal syndicate as more money is funnelled towards them.

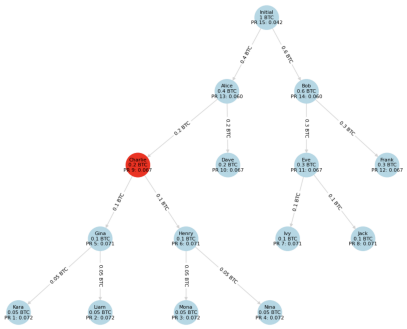

Figure 5: Example of a Money Laundering Network with PageRank Scores

Research has demonstrated the effectiveness of PageRank in detecting money laundering activities in Bitcoin networks. For example, Hu et al. (2019) explored the landscape of potential money laundering activities across the Bitcoin network using 4 different transaction classifiers with graph-based features: Immediate Neighbour-Based Classifier, Curated Features, Deepwalk and Node2Vec. Their study highlighted that laundering transactions could be differentiated from regular transactions based on various graph characteristics, such as network features like centrality measures, PageRank, and clustering co-efficient. By employing graph representation learning techniques such as node2vec, they achieved high classification accuracy of over 92%, demonstrating the potential of network-based features for AML detection as in Figure 6.

Sangers et al. (2020) introduced a secure multiparty PageRank algorithm for collaborative fraud detection between financial institutions. This approach allows multiple financial institutions to jointly compute PageRank values of their combined transaction graphs securely, using secure multiparty computation (MPC) techniques. By doing so, each institution can improve its fraud detection capabilities without compromising the privacy and confidentiality of its transaction data. Their experiments showed that this method is feasible for large-scale transaction graphs, with execution times scaling linearly with the number of nodes.

Table 2: Classifier Performance.

Classifier	Accuracy (%)	F1-measure
Neighbourhood	28.46	0.09
Manually extracted features	65.34	0.45
Deepwalk	91.72	0.94
Node2vec	92.05	0.94
“OR” ensemble	92.74	0.95
“AND” ensemble	21.47	0.02

Figure 6: Results from Transaction Classifiers[19]

In practical applications, PageRank-based AML detection can be integrated into machine learning models as a feature to enhance the identification of suspicious activities. The PageRank values, along with other graph-based features, can be used to add another evaluation metric to transactions flagged by existing classification techniques, reducing false positives and improving overall detection accuracy.

1.5 Other Limitations

Despite the benefits of transaction activity being publicly visible on the blockchain, certain limitations persist that can be exploited by illicit actors to launder money. One significant challenge is the lack of interoperability between different cryptocurrencies. For instance, if a customer sells Bitcoin and switches to Ethereum, tracing this movement becomes considerably more complex[4]. Each cryptocurrency operates on its own blockchain, with its own set of rules and transaction histories. While Bitcoin transactions can be tracked on the Bitcoin blockchain, and Ethereum transactions on the Ethereum blockchain, linking a transaction from one blockchain to another requires additional contextual information that may not be readily available. This complexity is

further compounded by the use of mixers and privacy-focused cryptocurrencies that obfuscate transaction paths, making it difficult to trace the origin and flow of funds[20].

Cross-chain activities often involve decentralised exchanges can facilitating the conversion of one cryptocurrency to another without leaving a clear, traceable record. In addition to this, cryptocurrency exchanges, services, or mixers based in jurisdictions with lax AML laws, inadequate KYC controls, or in sanctioned countries, often do not comply with international regulations. This lack of compliance removes visibility for regulators and law enforcement, further enabling illicit activities to go undetected[4]. Therefore, while blockchain technology provides transparency within individual networks, the lack of unified oversight and regulatory compliance across different blockchains and jurisdictions remains a significant hurdle in the fight against money laundering.

2 Research Questions

The aim of this research is to enhance the detection of money laundering activities within cryptocurrency networks by addressing three key research questions. These questions are structured around a three-step approach: transforming an existing dataset, understanding behavioural patterns and money laundering typologies, and building an ensemble algorithm. Addressing the below three research questions will aim to advance the detection and prevention of money laundering in a new and rapidly evolving landscape of cryptocurrency transactions:

1. How can a cryptocurrency transaction dataset be transformed to identify paths of Bitcoin transactions that include an illicit transaction?
2. What are common behavioral patterns of transaction paths which contain versus do not contain illicit transactions?
3. How can an algorithm be enhanced to detect a cluster of suspicious actors within the same transaction path?

2.1 Research Question 1 Objective

How can a cryptocurrency transaction dataset be transformed to identify paths of Bitcoin transactions that include an illicit transaction?

The first research question focuses on transforming the Elliptic++ [13] dataset to identify and visualise paths of Bitcoin transactions that do or do not involve illicit actors. This step is critical as it establishes a foundation for further analysis by constructing detailed datasets from which patterns of money laundering can be determined.

The Elliptic++ dataset is an enhancement of the original Elliptic dataset[11], providing additional information by including labelled actors (illicit, licit, and unknown). Detection at the actor level is necessary because actors can own multiple wallets, and therefore, identifying individual wallets alone is insufficient for comprehensive money laundering detection. The primary focus of this step is to transform the Elliptic++ dataset by extracting transaction paths from the initial node to the end node, including the different branches and the class of each actor involved (illicit, licit, unknown). By doing so, the full transaction dataset can be broken down into sub-networks or transaction paths, which can be individually visualised and analysed for money laundering typologies.

This first research question addresses a significant gap in current AML detection methodologies, which often fail to consider the interconnected nature of transactions and actors within a network. By focusing on the transformation of the dataset into sub-networks, this approach aims to provide a more holistic view of money laundering activities, enabling more effective detection and prevention strategies.

2.2 Research Question 2 Objective

What are common behavioral patterns of transaction paths which contain versus do not contain illicit transactions?

The second research question aims to understand the behavioural patterns and typologies of transaction paths that contain illicit transactions compared to those that do not. This involves conducting descriptive analysis

and exploratory analysis to identify similarities and differences within these paths. By analysing these patterns, legitimate and illicit transaction paths can be differentiated, providing a deeper understanding of the common traits of money laundering activities. This knowledge is essential for developing more effective detection strategies and improving the accuracy of existing models that are appropriate to money laundering on the blockchain.

The focus is on descriptive analytics to understand various aspects of these transaction paths created in Research Question 1, such as the density and length of the networks. Key metrics to be analysed include the number of nodes (actors) involved, the length of the transaction paths, the values of transactions, and other relevant characteristics. By examining these metrics, insights into the structure and behaviour of both licit and illicit transaction networks can inform which algorithms can be applied in Question 3.

For instance, the analysis will look at how many actors they are sending Bitcoin to, or receiving Bitcoin from, the number of wallets an actor may have depending on their class, and key features that may indicate whether a node is an individual or crypto service, such as a mixer. Mixers are often used to obfuscate transaction paths, making it difficult to trace the origin and flow of funds. Understanding the presence and behaviour of such services within the network is crucial for identifying illicit activities[20]. Additionally, the analysis will examine the speed of transfers within these networks. Rapid movement of funds between wallets can be indicative of money laundering layering techniques, where illicit actors attempt to obscure the origins of the funds through a series of quick, complex transactions. By comparing the speed of transfers in networks with and without illicit actors, we can identify patterns that are characteristic of money laundering activities.

Overall, the goal is to compare transaction paths containing illicit actors with those that do not (licit and unknown) to uncover distinctive behaviours and patterns. For example, networks involving illicit actors may exhibit higher density, with more interconnected nodes and shorter paths between them, reflecting a more coordinated effort to launder money. In contrast, licit networks may show more straightforward and transparent transaction paths.

By identifying these patterns, this research question seeks to uncover the underlying typologies of money laundering within cryptocurrency networks and whether they align or differ from existing research[20][3]. The insights from this analysis will inform how existing algorithms can be enhanced to provide better AML detection on the blockchain.

2.3 Research Question 3 Objective

How can an algorithm be enhanced to detect a cluster of suspicious actors within the same transaction path?

The third research question addresses the enhancement of algorithms to detect clusters of suspicious actors within a transaction path. The objective is to build and improve classification algorithms to capture multiple actors suspected of money laundering within the same transaction path. Traditional binary classification methods focus on identifying individual illicit actors, often missing the broader context of interconnected criminal networks.

The goal is to develop an ensemble algorithm that can operate in real-time on a live transaction dataset, which can be operationalised within an organisation. Previous research have applied models on complete datasets with good performance, however, in real-life application, there is incomplete data and unfolding networks. For this reason, this enhanced ensemble algorithm must be computationally efficient as to respond in a timely manner on growing transaction paths as the network unfolds. Binary classification serves the purpose of labelling nodes, but this can be enhanced with an algorithm that traverses the network and creates a significance score based on the transaction path and the importance within the sub-network.

This approach addresses a gap in existing research and AML programs in the industry, which typically focus on the classification of individual actors, ignoring their connections to other actors. By integrating network-based algorithms, such as PageRank, with binary classification, such as Random Forest, the enhanced algorithm aims to detect not just individual illicit transactions but also clusters of interconnected actors exhibiting suspicious behaviours.

As the desired outcome is to produce an ensemble algorithm that works in a real-life transaction monitoring, the desired output is to present investigators with a list of suspicious transaction paths including actors with

predicted classes in an order to investigate. Actors within each suspicious transaction path would be prioritised based on their PageRank score. This serves two primary purposes:

1. Capturing the Network: Identifying potential criminal syndicates by considering the entire transaction path rather than isolated actors.
2. Operational Efficiency: Providing investigators with a ranked list of transaction paths, and within it, a ranked list of actors to investigate, improving the efficiency and effectiveness of AML efforts.

By combining the strengths of binary classification and network analysis, the ensemble algorithm offers a more comprehensive solution to combating money laundering. It enhances detection capabilities by addressing the limitations of isolated detection methods and improving the ability to uncover complex money laundering schemes within cryptocurrency networks, while providing operational efficiencies.

3 Methodology

To address the research questions, a seven-step approach will be followed to analyse and enhance the detection of money laundering activities within Elliptic++ dataset. This methodology integrates data preprocessing, network analysis, behavioural pattern recognition, and algorithm development, with a key focus on the PageRank algorithm in conjunction with binary classification. The seven steps are as follows:

1. Preprocess the Dataset
2. Build Transaction Paths
3. Understand Behavioral Patterns
4. Filter Illicit Transaction Paths
5. Apply PageRank Algorithm
6. Develop an Ensemble Algorithm
7. Evaluation

3.1 Preprocess the Dataset

The initial step involves preprocessing the Elliptic++ dataset [13]to prepare it for analysis. This will include cleaning the data, handling missing values, and standardising the formats of transaction records to ensure consistency and accuracy. The Elliptic++ dataset is chosen as it includes labelled actors (illicit, licit, unknown), which is crucial for detection at the actor level, considering actors can own multiple wallets. As newer labelled datasets become available, these will be considered as an alternative dataset to Elliptic++. One consideration is the recently released Elliptic2 dataset[21].

3.2 Build Transaction Paths

Using the preprocessed dataset, transaction paths will be constructed to map the flow of Bitcoin between sending and receiving actors. This can be done using the NetworkX package to create these node-node directional connections, illustrating the flow of transactions within the network. This step involves extracting transaction paths from the initial node to the end node, including different branches and the class of each actor. This transformation is essential for breaking down the full transaction dataset into sub-networks or transaction paths, enabling detailed visualisation and analysis. Figure 7 is an example of a dataframe of different transaction paths using the NetworkX python package to traverse through the node-to-node dataset. Figure 8 is an example of a visualised transaction path containing an illicit actor.

	network_timestamp	network_name	length_of_network	actor_IDs	illicit_count	licit_count	unknown_count
40370	29	network_40371	202	[46085970, 165849645, 165849650, 165849653, 16...	184	16	2
40302	29	network_40303	199	[165849653, 165849656, 165849657, 124876736, 1...	181	16	2
40048	29	network_40049	191	[43878665, 165849931, 165849935, 165849938, 16...	173	16	2

Figure 7: Example of Transaction Paths

3.3 Understand Behavioural Patterns

An analysis will be conducted to understand the behavioural patterns of transaction paths containing illicit actors compared to those with licit actors. This step involves descriptive and exploratory analysis to identify similarities and differences, focusing on metrics such as the number of nodes, path lengths, transaction values, and the speed of transfers. By examining these metrics, insights into the structure and behaviour of both licit and illicit transaction networks can be gained. This analysis will look at various aspects, including the density of networks, the presence of crypto services like mixers, and the rapid movement of funds indicative of money laundering layering techniques.

3.4 Filter Illicit Transaction Paths

The dataset will then be filtered to isolate transaction paths that include illicit actors. This refined dataset will provide a focused view of potentially suspicious activities, allowing for more detailed analysis and modelling. Filtering on transaction paths containing illicit actors ensures that the subsequent analysis and algorithm development are targeted towards the most relevant parts of the dataset.

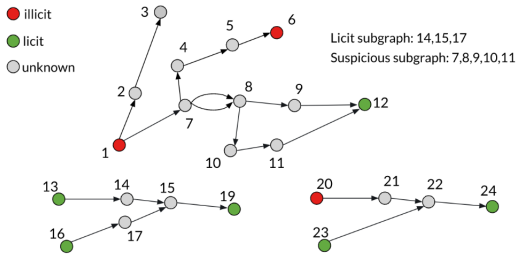

Figure 8: Example of Transaction Path with Illicit Actor[21]

3.5 Apply PageRank Algorithm

The PageRank algorithm, originally developed by Google to rank web pages, will be applied to rank actors within the transaction paths. PageRank operates on the assumption that more important nodes have more inbound connections[17]. In this context, it will help identify key actors in the money laundering network by highlighting nodes deeper in the transaction path where more significant amounts of money are funnelled. This ranking provides a score that reflects the relative importance or influence of each node within the network[16][18]. Figure 9 is an example of PageRank applied to a fictitious transaction path, with a suspicious transaction path highlighted in grey.

3.6 Develop an Ensemble Algorithm

An ensemble algorithm will be built that combines binary classification with the PageRank scores. This algorithm will first classify each node as either licit or illicit using a binary classification model, likely Random Forest due to its superior performance in handling imbalanced datasets[10][12]. Following classification, the PageRank scores will be used to rank the actors within the transaction path[16][19]. The integration of these two methods aims to enhance the detection capabilities by leveraging both node-based classification and network-based ranking. The algorithm must be capable of operating in real-time, providing timely responses to growing transaction paths as the network unfolds.

3.7 Evaluation

The evaluation of the methodology will be carried out using three sets of metrics:

1. **Binary Classification Metrics**: Accuracy, recall, and precision will be assessed, with a particular focus on recall due to the imbalanced nature of the dataset.

2. **Network Metrics**: Metrics such as node density and clustering will be analysed to determine the influence of nodes on each other and identify clusters of actors within the network.

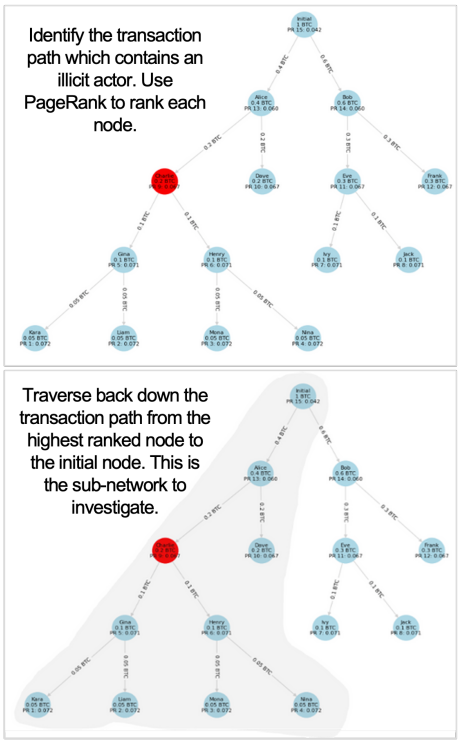

Figure 9: Example of PageRank Applied to a Transaction Path

3. **PageRank Metrics**: A threshold will be applied to identify the top n most significant nodes. The performance will be measured by checking if these top nodes are correctly labeled as illicit, using the same metrics as binary classification, with an emphasis on recall.

This 7-step approach will build an ensemble algorithm that not only helps identify illicit actors but also uncovers the potentially criminal networks they are involved in, with the final output producing a ranked list of suspicious transaction paths and the actors within them, prioritised for investigation.

4 Evaluation

Due to the application of different algorithms, multiple sets of evaluation metrics are employed in this study. These metrics help assess the performance and effectiveness of the proposed ensemble algorithm in detecting illicit activities within cryptocurrency networks.

4.1 Binary Classification of Illicit vs. Licit Actors

To evaluate the binary classification of illicit versus licit actors, the following metrics are used:

- **Accuracy**: The proportion of correctly identified illicit and licit transactions out of the total transactions evaluated. This metric provides a general sense of how well the model distinguishes between illicit and licit activities.
- **Precision**: The ratio of accurately identified illicit transactions to all transactions labelled as illicit. Precision is essential for minimising false positives, ensuring that the transactions flagged as illicit are truly suspicious, which is crucial for blockchain analysis where high false positive rates can overwhelm investigators.
- **Recall**: The fraction of actual illicit transactions correctly detected by the model. Recall measures the model's ability to identify all illicit activities within the blockchain network.
- **F1-Score**: A harmonic mean of precision and recall, the F1-Score balances the trade-off between these two metrics, indicating the model's overall accuracy in detecting illicit transactions.

4.2 Network Metrics for Transaction Paths

To understand the density and centrality within the transaction paths, the following network metrics are considered:

- **Degree Centrality**: Measures the number of edges connected to a node, indicating the node's involvement and connectivity within the network. High degree centrality may suggest significant activity and potential importance in the network.
- **Betweenness Centrality**: Measures the number of times a node acts as a bridge along the shortest path between two other nodes, highlighting its control over information flow. Nodes with high betweenness centrality are critical for the dissemination of transactions.
- **Closeness Centrality**: Measures how close a node is to all other nodes in the network, suggesting its ability to quickly interact with others. This metric can identify influential nodes within the network.
- **Eigenvector Centrality**: Measures a node's influence based on the principle that connections to high-scoring nodes contribute more to the score of the node in question. This helps in identifying influential nodes that are well-connected to other influential nodes.
- **Modularity**: Assesses the structure of network clusters by comparing the density of edges inside clusters to edges between clusters. High modularity indicates strong community structures, which may be indicative of organised groups.
- **Clustering Coefficient**: Measures the likelihood that two adjacent nodes of a node are connected, providing insight into the clustering level of the network. High clustering may indicate close-knit groups or sub-networks within the larger network.

4.3 PageRank Metrics

To evaluate the effectiveness of the PageRank algorithm in ranking the importance of actors within the transaction paths, the following classification metrics are applied after a threshold of the top x ranked nodes is applied:

- **Accuracy**: Evaluates the overall correctness of the ranking by comparing the identified top nodes with actual illicit nodes.
- **Precision**: Measures how many of the top-ranked nodes are actually illicit, which is crucial for ensuring that the most significant nodes flagged for investigation are truly suspicious.
- **Recall**: Assesses the proportion of actual illicit nodes that are correctly identified among the top-ranked nodes, ensuring comprehensive detection within the top ranks.
- **F1-Score**: Provides a balanced measure of precision and recall, indicating the overall effectiveness of the PageRank algorithm in identifying important illicit nodes.
- **Area Under the Curve (AUC)**: Evaluates the performance of the classification model over all classification thresholds, providing a single metric that balances the trade-offs between true positive and false positive rates.

This multi-set evaluation approach ensures that the proposed ensemble algorithm is thoroughly tested and validated. By assessing multiple dimensions of performance, including binary classification accuracy, network metrics, and the effectiveness of the PageRank algorithm, this study aims to provide a robust and reliable solution for detecting illicit activities in cryptocurrency networks.

5 Conclusion

The motivation for this research project stems from the growing need to effectively combat money laundering that occurs in both traditional banking systems and cryptocurrency networks.

Traditional banking systems have established various AML programs and legal frameworks, such as the Bank Secrecy Act in the United States and the Anti-Money Laundering and Counter-Terrorism Financing Act in Australia, which mandate strict compliance requirements for financial institutions. These include Know Your Customer (KYC) procedures, transaction monitoring, and reporting of suspicious activities. However, the traditional AML approaches often rely on rule-based models that struggle to keep pace with the sophisticated tactics of modern money launderers. In the context of cryptocurrency, the challenges are even more pronounced. The pseudonymous nature of blockchain transactions, the lack of unified oversight across different blockchains, and the presence of non-compliant exchanges in jurisdictions with lax regulations create significant obstacles for AML efforts. Current detection methods on the blockchain often focus on binary classification of individual transactions or actors, which can miss the broader network of illicit activities. These limitations highlight the urgent need for more advanced and comprehensive AML detection techniques.

This research proposes an innovative approach to address these gaps by developing an ensemble algorithm that combines binary classification with the PageRank algorithm. This combined approach aims to not only identify individual illicit actors but also uncover the potentially criminal networks they are part of. A key aspect of this research is the focus on real-time application. The proposed ensemble algorithm is designed to operate on live transaction datasets, dynamically responding to unfolding networks and providing timely detection of suspicious activities. By presenting investigators with a prioritised list of suspicious transaction paths and actors, this method enhances the efficiency and effectiveness of AML operations resulting in a time and cost saving.

This research contributes to the field of AML detection by introducing a novel ensemble algorithm that leverages the strengths of both binary classification and network analysis. By addressing the current limitations and focusing on real-time applicability, this approach offers an advancement in the detection and prevention of money laundering in cryptocurrency networks. The ultimate goal is to create a more resilient and efficient AML system that can adapt to the evolving landscape of financial crime, thereby safeguarding the integrity of financial systems worldwide.

References

[1] McKinsey, *The fight against money laundering: Machine learning is a game changer*, Accessed: 2024-05-30, 2024. [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer.

[2] AUSTRAC, *Transaction monitoring*, Accessed: 2024-05-30, 2024. [Online]. Available: https://www.austrac.gov.au/business/core-guidance/amlctf-programs/transaction-monitoring.

[3] AUSTRAC, *Money laundering in australia 2011*, Accessed: 2024-05-30, 2011. [Online]. Available: https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/money-laundering-australia-2011.

[4] S. Gruber, "Trust, identity and disclosure: Are bitcoin exchanges the next virtual havens for money laundering and tax evasion," *Quinnipiac Law Review (QLR)*, vol. 32, no. 1, 135–[ii], 2013. [Online]. Available: https://heinonline.org/HOL/P?h=hein.journals/qlr32&i=143.

[5] P. of Australia, *Amlctf act 2006*, Accessed: 2024-05-30, 2001. [Online]. Available: https://www.legislation.gov.au/C2006A00169/latest/text.

[6] AUSTRAC, *Aml ctf programs*, Accessed: 2024-05-30, 2024. [Online]. Available: https://www.austrac.gov.au/business/core-guidance/amlctf-programs.

[7] M. Jullum, A. Loland, R. B. Huseby, G. Anonsen and J. Lorentzen, "Detecting money laundering transactions with machine learning," *Journal of Money Laundering Control*, vol. 23, no. 1, pp. 19–33, 2020, Open Access. Article publication date: 21 January 2020. Issue publication date: 27 January 2020. DOI: 10.1108/JMLC-07-2019-0055. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/JMLC-07-2019-0055/full/html.

[8] Financial Crimes Enforcement Network, *Bank secrecy act*, Accessed: 2024-05-31, 2024. [Online]. Available: https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act.

[9] Coinpaper, *Crypto exchanges without kyc: How to find a privacy-friendly cryptocurrency exchange*, Accessed: 2024-05-31, 2024. [Online]. Available: https://coinpaper.com/3756/crypto-exchanges-without-kyc-how-to-find-a-privacy-friendly-cryptocurrency-exchange.

[10] M. Weber, G. Domeniconi, J. Chen *et al.*, "Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics," 31 Jul. 2019. [Online]. Available: http://arxiv.org/abs/1908.02591 (visited on 04/04/2024).

[11] "Elliptic data set." (), [Online]. Available: https://www.kaggle.com/datasets/ellipticco/elliptic-data-set (visited on 01/04/2024).

[12] Y. Elmougy and L. Liu, "Demystifying Fraudulent Transactions and Illicit Nodes in the Bitcoin Network for Financial Forensics," in *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, 6 Aug. 2023, pp. 3979–3990. DOI: 10.1145/3580305.3599803. arXiv: 2306.06108 [cs]. [Online]. Available: http://arxiv.org/abs/2306.06108.

[13] "Elliptic++ dataset." (), [Online]. Available: https://github.com/git-disl/EllipticPlusPlus (visited on 18/04/2024).

[14] N. Beheshti, "Random forest classification: Background information & sample use case in 7 minutes," *Towards Data Science*, Jan. 2022, Accessed: 2024-05-31. [Online]. Available: https://towardsdatascience.com/random-forest-classification-678e551462f5.

[15] NetworkX Developers, *Networkx documentation: Examples*, Accessed: 2024-05-31, 2024. [Online]. Available: https://networkx.org/documentation/latest/auto_examples/index.html.

[16] A. Sangers, M. van Heesch, T. Attema *et al.*, "Secure multiparty pagerank algorithm for collaborative fraud detection," in *Financial Cryptography and Data Security. FC 2019. Lecture Notes in Computer Science*, I. Goldberg and T. Moore, Eds., vol. 11598, Springer, Cham, 2019, pp. 679–698. DOI: 10.1007/978-3-030-32101-7_35.

[17] Computerphile, *Page ranking and search engines - computerphile*, Accessed: 2024-05-26, 2024. [Online]. Available: https://www.youtube.com/watch?v=v7n7wZhHJj8&ab_channel=Computerphile.

[18] DataWorks Summit, *Using pagerank for fraud detection in healthcare data*, Accessed: 2024-05-26, 2024. [Online]. Available: https://www.youtube.com/watch?v=QtT3xCeifyY&ab_channel=DataWorksSummit.

[19] Y. Hu, S. Seneviratne, K. Thilakarathna, K. Fukuda and A. Seneviratne, "Characterizing and detecting money laundering activities on the bitcoin network," *arXiv preprint arXiv:1912.12060*, 2019.

[20] "The Chainalysis 2024 Crypto Crime Report." (), [Online]. Available: https://go.chainalysis.com/crypto-crime-2024.html (visited on 18/03/2024).

[21] C. Bellei, M. Xu, R. Phillips *et al.*, "The shape of money laundering: Subgraph representation learning on the blockchain with the elliptic2 dataset," *arXiv preprint arXiv:2404.19109*, 2024. [Online]. Available: https://doi.org/10.48550/arXiv.2404.19109.