National College of Ireland

# Leveraging Graph Convolutional Networks for the Detection of Illicit Bitcoin Transactions

MSc Research Project
Data Analytics

Kavitha Kannekanti
Student ID: x23237422

School of Computing
National College of Ireland

Supervisor: Cristina Hava Muntean

**National College of Ireland**

**MSc Project Submission Sheet**

**School of Computing**

**Student Name:** Kavitha Kannekanti

**Student ID:** X23237422

**Programme:** Msc Data Analytics **Year:** 2024 - 2025

**Module:** Msc Research Project

**Supervisor:** Cristina Hava Muntean

**Submission Due Date:** 29/01/2025

**Project Title:** Leveraging Graph Convolutional Networks for the detection of Illicit Bitcoin Transactions.

**Word Count:** 9822 **Page Count:** 22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

**Signature:** K.Kavitha

**Date:** 29/01/2025

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST**

| | |
|---|---|
| Attach a completed copy of this sheet to each project (including multiple copies) | □ |
| **Attach a Moodle submission receipt of the online project submission,** to each project (including multiple copies). | □ |
| **You must ensure that you retain a HARD COPY of the project**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. | □ |

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

| **Office Use Only** | |
|---|---|
| Signature: | |
| Date: | |
| Penalty Applied (if applicable): | |

# Leveraging Graph Convolutional Networks for the Detection of Illicit Bitcoin Transactions

Kavitha Kannekanti
X23237422

**Abstract**

With the advancement of cryptocurrencies, especially Bitcoin, the rate and instances of crimes have increased to become a challenge to the agencies responsible for regulation. The heuristic techniques, which are commonly used in detecting frauds are traditional methods, take a lot of time and cannot be easily scaled. This research proposes a new approach called Graph-based Transaction Anomaly Detection (GTAD) that employs Graph Convolutional Networks (GCNs), Temporal Graph Convolutional Networks (T-GCNs) and transformers to enhance the identification of Illicit Bitcoin transactions. For the modelling of Bitcoin transaction networks, GTAD builds a directed graph where temporal dynamics are associated with time-based snapshots. For feature learning, this approach employs GCNs to extract meaningful node embeddings, while temporal attention helps identify important temporal and spatial patterns in transaction data. Also, the hierarchical attention mechanism gives preference to massive transactions and concentrates on areas of high fraud risk. The proposed model is trained under supervised learning paradigm, with a weighted cross entropy loss function to handle class imbalance. Comparing GTAD with various machine learning methods for detecting illicit activities shows that GTAD provides higher accuracy and better scalability. The performance of the GTAD is higher than that of other models with 98.49% accuracy and 0.94 macro F1-score. These findings demonstrate the applicability of the model to prevent financial crimes in the cryptocurrency context and can help improve the detection of fraud in the constantly developing digital currency environment.

Keywords: Fraudulent Transactions, Graph-based Transaction Anomaly Detection (GTAD), Graph Convolutional Networks (GCNs), Bitcoin transactions

# 1 Introduction

Cryptocurrencies have especially Bitcoin expanded rapidly in the financial markets across the globe in recent years. Bitcoin has been considered a revolutionary digital currency because of its decentralized structure, better privacy, and security measures in its transaction processing. Nevertheless, like every other digital currency, Bitcoin has been associated with so many benefits but also carries the tag of being an ideal tool for criminal businesses such as money laundering, terrorism funding, and fraudsters. The key issues that make the use of Bitcoin dangerous include; First, Bitcoin has anonymity, which makes it hard for the regulatory body and the police to track the perpetrators of the frauds Second, once the fraud is executed, it is irreversible, therefore the victims cannot recover their money. Most of the existing approaches for identifying fraudulent transactions in Bitcoin networks are heuristic based and

rule-based approaches. Although these methods have given some level of usability, they have certain drawbacks which are very crucial. In particular, they are time-consuming, cannot be easily integrated with the increasing volume of transactions, and prove to be ineffective in addressing the dynamic nature of fraud schemes. Since the adoption of Bitcoin increases, the complexity of the crimes rises, and thus, there is a need for better and more flexible methods of fraud prevention.

Recently, graph-based methods together with machine learning methods show promising results in detecting frauds in the transaction networks (Valem et al., 2023; Shah et al., 2023). These models can capture relational and structural characteristics as Bitcoin transactions are presented as graphs where nodes are the wallets, and edges are the transactions. However, the current graph based models which we inherit still have some drawbacks in terms of handling the temporal aspect of the transactions, scalability issues with large data sets and the identification of the important transaction patterns which are precursors of the potential fraudulent transactions. To this end, this research seeks to fill these gaps through the development of a new approach for the detection of illicit bitcoin transactions known as GTAD- Graph-based Transaction Anomaly Detection which incorporates Graph Convolutional Networks (GCNs), Temporal Graph Convolutional Networks (T-GCNs) and transformers.

The purpose of this research is motivated by the fact that existing techniques used to detect fraud in Bitcoin networks have their drawbacks. Existing models are not well suited for large scale and dynamic networks where such malicious behaviors are masked in layers of interactions. The problem with this approach is that traditional methods that rely on manually designed heuristics cannot adapt to higher dimensions and changes in scale easily, and many current machine learning methods do not incorporate the temporal nature of transactions in the Bitcoin system. However, graph-based models, despite being superior to the previous models in terms of capturing the structural properties of the transaction networks, do not possess the necessary components of capturing the most important regions, such as the areas with high frequency of illicit transactions. There is a growing need for a model that can not only understand the structural and temporal properties of these network but also rank the transactions that are more suspicious in order to increase the accuracy of detection. This gap leads to the creation of a more elaborate, expandable, and flexible solution that will involve GCNs, transformers, and temporal analysis to enhance identification of licit & Illicit transactions in Bitcoin.

## Research Question

This research study aims to explore the following key research question:

> **"How effectively can proposed GTAD model outperform the baseline models including the Logistic Regression, Decision tree and Random Forest?"**

Addressing these questions is crucial for enhancing our understanding of fraudulent activity patterns in Bitcoin transactions and improving the detection capabilities of graph-based models.

## Objective:

The main aim of this research study is design and implement the GTAD (Graph-based Transaction Anomaly Detection) model, which employes the Graph Convolutional Networks (GCNs) and transformers to recognize the illicit type of Bitcoin transactions. Specifically, the research aims to achieve the following:

**Graph Construction:** Construct directed graphs depicting Bitcoin transaction networks and incorporate temporal knowledge by constructing temporal snapshots. These graphs will help in providing structural representation of transaction network and will help in identifying relationship and pattern similar to fraud.

**Temporal Attention with Transformers:** Add transformers to incorporate self-attention mechanisms that capture temporal and spatial dependencies in the transaction graph. With transformers, further improvements will be made so that the model can pay attention to the dynamic aspect of illicit transactions, new fraudulent behaviors.

**Hierarchical Attention for Anomaly Detection:** Incorporate hierarchical attention mechanisms to input attention map for prioritizing transactions within the network by focusing on the significant regions of the model—like hotspots of fraud transactions. This will make it easier to identify the prohibited operations to increase the effectiveness of their prevention.

**Model Evaluation and Benchmarking:** Therefore, the next step is to assess how the GTAD model performs against classical methods and other GNN methods that exist in literature. The performance of the proposed model will be evaluated by F1-score, precision, and recall measures; it will be aimed to prove the higher scalability and accuracy of identifying illicit transactions in the massive Bitcoin network using the proposed approach in comparison with the related works.

## Research Study Structure

The study is divided into a number of significant parts as follows. In Section 2, related works on cryptocurrency transaction detection, the use of graph-based models, and the application of GCNs and transformers for anomaly detection are reviewed. Section 3 features the proposed approach, the Graph-based Temporal Anomaly Detection (GTAD) model. This section describes the construction of the graph, the generation of GCN embeddings, the incorporation of temporal attention mechanisms, and the hierarchical attention mechanism used for anomaly detection. Section 4 is devoted to the presentation of the experimental results & discussion, where the metrics for evaluation and the datasets used are presented, as well as the comparison of the performance of the proposed GTAD model with other existing methods. Where the detailed discussion and analysis of the experimental findings, while emphasizing on what the authors considered to be one of the strengths of the GTAD model, and the limitations of it. Lastly, Section 5 provides the conclusion where the main results and

implications of the research are outlined along with the possible directions for further studies aimed at enhancing the capability to identify illicit activities within cryptocurrencies.

# 2 Related Work

The emergence of cryptocurrencies, especially Bitcoin, has disrupted financial systems around the world. However, due to its decentralised and somewhat pseudonymous structure, it has also attracted a number of unlawful uses, such as money laundering, fraud and ransomware payments (Olsson et al., 2024; Nicholls et al., 2023). To protect the credibility and security of blockchain technologies, it is essential to notice these illicit operations. The previous approaches applied to identify frauds in the financial sector, for instance, rule-based systems, are ineffective because frauds in the more complex and diverse cryptocurrency networks require new approaches (Fahmi et al., 2023). This literature review provides a critical analysis of the development of methods for identifying fraudulent transactions within Bitcoin networks, primarily graph-based approaches and Machine Learning techniques like GCNs, T-GCNs, and transformers. It seeks to present the research gap that this section has established and the need to develop the Graph-based Transaction Anomaly Detection (GTAD) model presented in this thesis.

## 2.1 Illicit Activities in Bitcoin Networks

Bitcoin's architecture is open, and the decentralized structure has made it the go-to asset for unlawful illicit type of activities. Another important issue in cryptocurrency networks is the identification of such fraudulent transactions since the number of such operations is enormous and continually increasing, and criminals are constantly improving their methods (Olsson et al., 2024). The early works in this context used heuristic and rule-based systems where the system highlighted the suspicious transactions using the predefined limit, including the transaction value or the number of connections in the network (Fahmi et al., 2023; Nicholls et al., 2023). However, these methods are not enough scalable and flexible to address the growing and changing nature of fraudulent behaviours in Bitcoin networks. Also, rule-based systems are likely to produce many false alarms, which is likely to flag genuine transactions as suspicious.

## 2.2 Graph-Based Approaches for Fraud Detection

In the last few years, graph-based approaches have emerged as an effective paradigm for detecting suspicious activities in transaction networks, particularly in the context of Bitcoin and other cryptocurrencies. These approaches represent transactions as graphs, where nodes are specific objects: wallets or accounts, and edges are transactions between them. This makes the capturing of transaction relations and interactivity possible, which is a better approach than the traditional methods (Bhatti et al., 2023; Mir & Musa et al., 2023). They enable it to identify multi-phase fraud scenarios and other connections between fraudulent parties that are often very hard to identify in other ways. The graph-based model proves useful for identifying an anomalous behaviour because it can capture changes in the nature of

the nodes' interactions within a TNM model. In contrast to rule-based approach or statistical, the graph-based approaches allow to identify fraud scenarios which involve more than one link, or a stage, or the fraudster has relationships with several other parties. For example a set of transactions which may have looked suspicious to the users or the system may not be easily identifiable each time while observing the whole interactions then the problem can easily be identified. The decision to analyze the transaction network in its entirety as an overall approach significantly enhances the effectiveness of identifying fraud cases (Bhatti et al., 2023).

One of the most common methods of working with graph data is the GCNs, with which there is a high accuracy in solving fraud detection problems (Valem et al., 2023; Lee et al., 2024). GCNs achieve this by convolving the nodes and the neighbors of the graph in such a way that the model can be able to learn the local and the overall transactions. This allows GCNs to easily focus on potentially fraudulent actions because the structure provides insight into the occurrence of illicit actions such as money laundering or acting on network (Nie & Li et al., 2023). The major advantage of GCNs is that the structure of a graph can be used to detect fraud that may have related entities or transactions. Furthermore, we have seen that GCNs are capable of capturing structural evidence of fraudulent behaviors that are usually attributed to certain and unusual forms of transactions or flows. In this way, GCNs can warn a company of a fraud even if it is low level or if it is spread out in between several accounts. Prior works have established that GCNs can be applied to detect fraud inside transaction structures and has established that GCNs can capture patterns that are not discernible in other ways (Valem et al., 2023; Lee et al., 2024). In conclusion, the graph-based methods, particularly GCNs, are more effective compared to the prior methods for fraud detection and gives a richer and engaged perspective of the transaction graph. Since these models are based on analyzing the relations between the entities and the money flow, these models can identify the multilevel fraud schemes, which are not identified by the traditional methods; thus, these models are the perspective for protection of the financial systems from fraudulent activities.

## 2.3 Temporal Graph Convolutional Networks (T-GCNs) & Transformers and Attention Mechanisms

While the GCNs have a good capability in analyzing the fixed graph, their performance is relatively poor in analyzing a graph over time. In Bitcoin transaction networks, the malicious behaviors have different temporal properties, for instance, spike activity or high density in the transaction frequency in small time periods (Shah et al., 2023; Alarab et al., 2024). These temporal dependencies are challenging to incorporate for static graph models so that fraud can be easily detected. To overcome this, Temporal Graph Convolutional Networks (T-GCNs) has been invented which integrates temporal information into graph based models. T-GCNs have been used effectively in many areas such as traffic prediction (Nie & Li et al., 2023) and financial fraud detection because detecting temporal-sensitive anomalies is crucial for accurate fraud identification. Hence, the T-GCNs enhance the capacity of the traditional GCNs that can only detect the spatial relation between entities (i.e., how they are connected) and the temporal relations which are important to understand how these illicit activities are evolved over time. Incorporation of time-based snapshots of the transaction network in T-

GCNs enhances the learning patterns of GCNs. This is even truer for Bitcoin as it may take scammers some amount of time to ramp up their work or they may have bursts of activity, meaning that the work needs both temporal and spatial analysis. Hence, it becomes possible for T-GCNs to offer a better solution as compared to the existing static models in modeling dynamic fraud patterns which the later cannot capture.

A recent advancement in the application of the machine learning paradigm for anomaly detection on graphs is transformers and attention mechanisms. Initially introduced by Vaswani et al. (2017), the transformers utilize self-attention to model long dependencies in data and are therefore suitable for sequence data processing. Regarding the Bitcoin transaction networks, the attention mechanisms will assist the model in focusing on the nodes (entities) or edge (transactions) that are most likely to engage in the frauds (Huang et al., 2023). This capability makes the model ideal to detect anomalies that would be otherwise hidden because the transaction graphs are complicated and large. Accordingly, Graph Attention Networks (GATs), which were proposed by Huang et al. (2023), can be considered as a development of GCNs, where the latter uses both node- level and graph-level attention. This is because the use of GATs allows the model to scale the output of nodes and edges, which are capable of capturing detailed differences in the patterns of transactions. This is especially useful in fraud detection where most of the fraud activities would be perceived to slightly manipulate the network. In this manner, GATs improve the model's capacity for focusing on proportional to the irregularity, and thus, decreasing the attention weights based on the node or edge relevance. Moreover, the hierarchical attention mechanisms can be applied again to zoom in on the particular subgraphs which might contain the fraud zones or the group of accounts that are engaged in the same fraud schemes. This is even more beneficial to the model as it is able to give attention to the specific parts of the graph and be able to capture easily missed fraud patterns.

## 2.4 Challenges with Comparison in Existing Approaches

However, some issues are still with graph-based and machine learning models to address illicit Bitcoin transactions. I think the first major limitation is the inability to scale up the use of the system. For large and complex transaction networks in the Bitcoin environment, models must handle a large amount of data; meanwhile, the detection accuracy cannot be compromised. All modern models face the problem of inefficiency when scaling, which causes problems with performance (Nie & Li et al., 2023). The third issue is the ability to apply existing models to newly emerging forms of fraud activities. Criminals always adapt to new ways of committing their crimes, thus, models trained on the historical data cannot predict new forms of frauds (Olsson et al., 2024). Moreover, many models do not have a clear explainability mechanism and, therefore, decision-makers, including regulators and law enforcement agencies, cannot rely on their results. This is especially so in areas of high risk such as cryptocurrency, where false positives can result in the bona fide accounts being frozen unfairly.

In order to give a better structured overview of the different approaches presented in the papers for the detection of illicit Bitcoin transactions this part offers a comparison of the most important research papers. To facilitate the comparison of the studies, they are

presented in tabular form, where one can find the authors, methodologies used, models implemented, metrics measured, limitations of the studies, and the authors' suggestions for future work.

**Table 1: Comparison between Existing Recent Researches**

| Authors | Methodology | Model Used | Limitations | Future Work |
|---|---|---|---|---|
| **Olsson et al. (2024)** | Analysis of illicit Bitcoin flows using a manual heuristics-based approach. | Heuristic-Based Detection Model | High false-positive rate, lacks scalability for large datasets. | Proposes automation using machine learning for enhanced scalability. |
| **Fahmi et al. (2023)** | A comprehensive survey of security and privacy issues in Bitcoin, with focus on transaction monitoring. | Rule-Based Fraud Detection | Inefficient in detecting evolving fraud patterns, relies on fixed rules. | Suggests dynamic learning models that adapt to new fraud patterns in real-time. |
| **Valem et al. (2023)** | Semi-supervised learning on graph data using convolutional networks. | Graph Convolutional Networks (GCNs) | Focuses on static graphs, lacks temporal data analysis. | Proposes integration of temporal dynamics to enhance GCNs for time-sensitive applications. |
| **Shah et al., (2023)** | Analysis of the temporal nature of fraudulent Bitcoin transactions and its impact on detection efficiency. | Temporal GCN (T-GCN) | Limited scalability with large transaction volumes, difficult to interpret the results. | Suggests implementing multi-scale GCNs to handle both large datasets and provide interpretable outputs. |
| **Bhatti et al. (2023)** | Extension of GCNs for relational data modeling with an emphasis on graph-based machine learning. | Relational Graph Convolutional Networks | Does not incorporate attention mechanisms, struggles with long-range dependencies in large graphs. | Proposes exploring attention-based models to better capture long-term dependencies in large-scale networks. |
| **Huang et al. (2023)** | Introduced Graph Attention Networks (GATs), applying self-attention to graph-based tasks. | Graph Attention Networks (GATs) | High computational cost, lacks scalability for large-scale graph networks. | Recommends optimizing computational efficiency for GATs to make them more scalable and applicable to large datasets. |
| **Nie & Li et al. (2023)** | Focused on time-series prediction using graph-based models with temporal and spatial data. | T-GCN, Temporal Graph Models | Only suitable for short-term time-series predictions, limited interpretability of learned patterns. | Future work includes extending T-GCNs for long-term prediction tasks and improving interpretability. |
| **Vaswani et al. (2017)** | Introduced the transformer model, revolutionizing sequence-based tasks with self-attention mechanisms. | Transformer | Lacks direct application to graph-based fraud detection tasks. | Suggests adapting transformer architectures for graph-based fraud detection with multi-attention mechanisms. |

## Conclusion

The literature shows an emerging trend of using sophisticated machine learning techniques for fraud detection in cryptocurrency networks. Although methods such as GCNs and T-GCNs have been proven to be useful, the application of these involves some limitations such as scalability and flexibility. Such shortcomings can be addressed by the integration of GCNs

with other architectures for instance the transformers. The idea for the novel GTAD model is an extension of this concept by incorporating temporal information and hierarchical attention to improve the detection of malicious nodes and address the scalability issue in Bitcoin transaction networks. In this way, GTAD intends to fill the main gaps outlined in the literature review and join the fight against illicit activities in the context of cryptocurrencies.

# 3 Research Methodology

This section presents the systematic approach and the technical approach taken in the development of the GTAD (Graph-based Transaction Anomaly Detection) model for identifying the illicit Bitcoin transactions. The approach is meant to provide for a proper and sequenced model development process, from the data collection and preparation, model development, training, and evaluation, to the final result interpretation as the outline of the research methodology is illustrated in Figure 1. To facilitate an understanding of how the study was conducted and how the proposed model was implemented and validated, each stage is discussed in detail below.

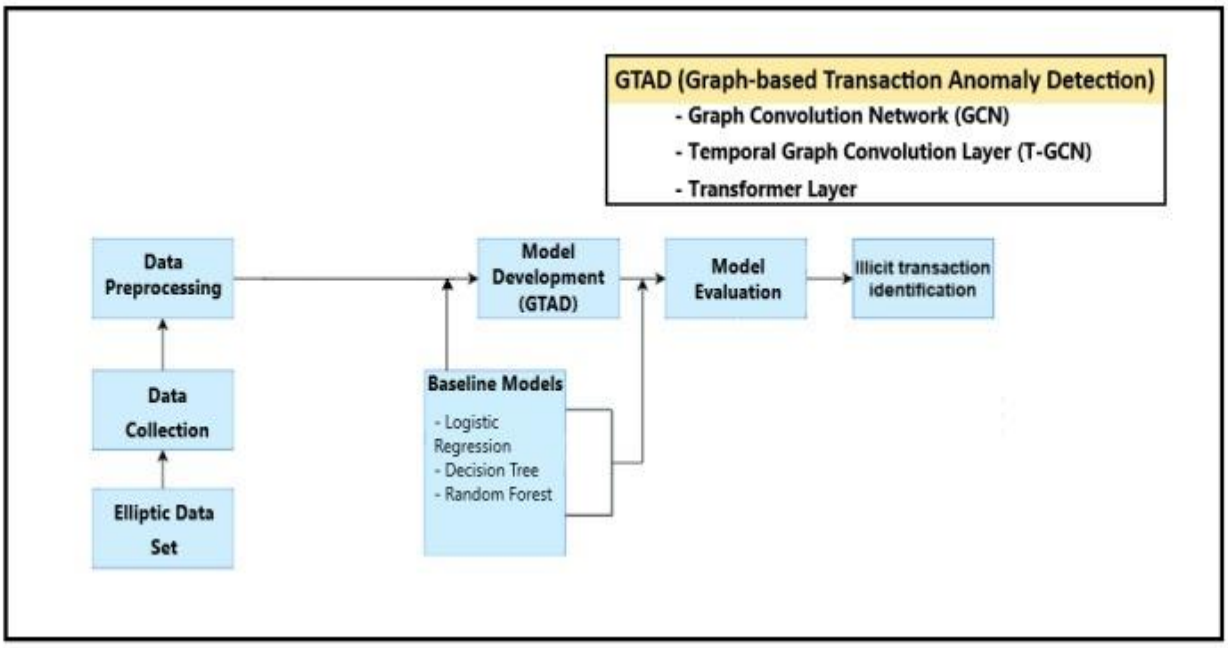



**Figure 1: Methodology for Illicit Bitcoin Transaction**

## 3.1 Dataset

The dataset employed in this research, to explore and analyze is the Elliptic Data Set obtained from Kaggle and comprises of Bitcoin transactions (Weber, M., et al., 2019). This dataset is very useful in identifying the flow and activity in the Bitcoin network so that we are able to identify the illicit flows within the network. The dataset comprises three primary parts:

**Features:** Characteristics of the Bitcoin transactions.
**Classes:** Two classes of labels that describe the nature of transactions as either illicit, licit or if the information is unknown.

**Edgelist:** These are the representations of the relationships (transactions) that exist between Bitcoin addresses.

**Dataset Overview**

The GTAD model dataset includes several components that are aimed at reflecting both the transactional and behavioral characteristics of Bitcoin addresses. The Features Data has a total of 203,769 rows and 167 columns which include time stamps, amount of transactions and other features that characterizes temporal and transactional behavior of bitcoin addresses as represented in Figure 2. These features are used to create the transaction graph and to train the machine learning model, as the features deliver valuable information about the transactions.

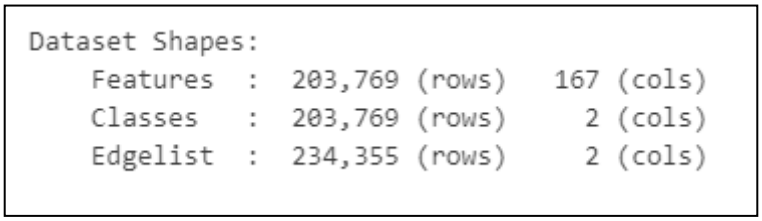



**Figure 2: Shapes of Dataset**

Besides the features, Classes Data comprise 203,769 rows and 2 columns, which represent the class labels for transactions. The last class labels represent the nature of a transaction, namely, licit (legal), illicit (illegal), or of unknown status. The distribution of these labels is highly imbalanced, where the Unknown label accounts for 157,205 transactions (77.15%), Licit for 42,019 transactions (20.62%) and Illicit for 4,545 transactions (2.23%). Such distribution is due to the fact that it is difficult to identify the abnormal transactions as they are a small subset of all transactions. The Edgelist has 234355 rows and 2 columns as these contain the relations between the nodes in the graph. Each node represents a Bitcoin address while each edge is a transaction between two addresses. With the total of 203769 nodes and 234355 edges, of which 7297 are connected, the dataset represents the network of Bitcoin addresses and their transactions. For instance, we have the giant component of nodes 400 and edges 431, which shows the largest connected subgraph for the given Bitcoin transaction network. Such structure of the dataset is appropriate for analysis of spatial and temporal patterns of Bitcoin transactions in the GTAD model.

## 3.2 Graph Construction

The core of the GTAD model involves constructing a directed graph $G = (V, E)$ based on the Bitcoin transactions:

### 3.2.1 Nodes and Edges

**Nodes:** In the graph, each node is a Bitcoin address, which may be different from every other address. This leads to 203,769 nodes; all the entities that are involved in transactions as shown in figure 2 below. Directed edges are defined by the transaction flows and these are 234,355 edges are shown in figure 3. An edge from node to node means that address from which Bitcoin was sent is address

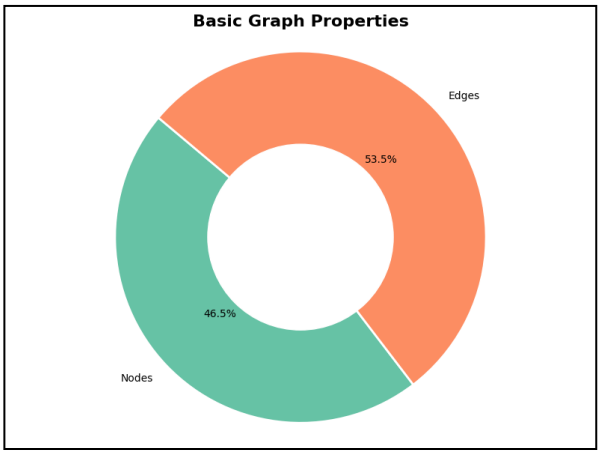



**Figure 3: Distribution of Basic Graph Properties**

**Edges:** Directed edges are established based on the transaction flows which are 234,355 **edges** are presented in Figure 2. An edge from node $A$ to node $B$ indicates that address $A$ sent Bitcoin to address $B$. The creation of edges enables the representation of relationships and transaction patterns within the graph.

### 3.2.2 Temporal Snapshots

To incorporate the temporal dimension of transactions:
The directed graph is partitioned into the time-based snapshots $G_t$, demonstrating the state of the graph at defined intervals. This enables the model to analyze transaction behaviors that how it evolves over time, while recognizing the trends and anomalies associated with illicit activities.

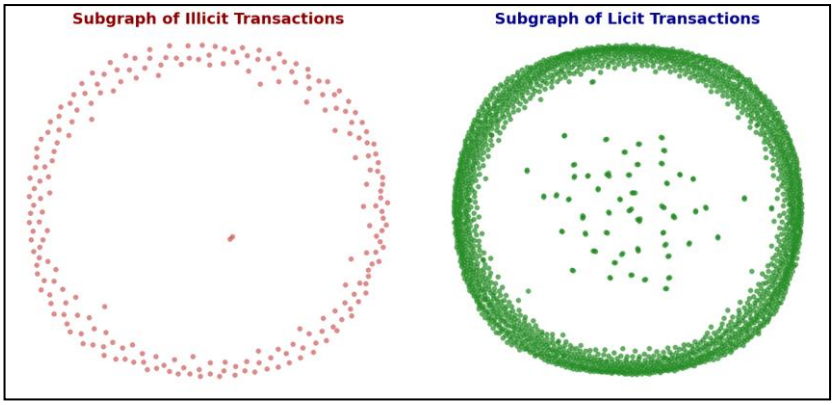



**Figure 4: Class based illicit and licit transactions**

In figure 4, plots of subgraphs for illicit and licit bitcoin transactions are shown. The nodes of the illicit transaction are sparse and isolated, which could represent the limited connectivity between entities. This pattern might suggest that illicit transactions are designed to minimize links with others to reduce traceability. The nodes of licit transactions of bitcoin are denser and more interconnected, forming a cluster. This likely indicates frequent and legitimate interactions between entities, reflecting normal transaction behaviour.

## 3.3 Data Preprocessing

Data preprocessing is a set of operations that prepare the extracted data for analysis using the graph-based machine learning models suitable for Bitcoin transaction data. Data Cleaning, the first process of the proposed approach, helps to perform further analysis by eliminating

the transactions that are invalid, contain missing values, or are replicated. The transactions with missing address, amount or time stamps are rejected to keep the quality of data and to feed the machine learning algorithm with good data.

Data cleaning is done before and after that Graph Construction is done and the cleaned data is converted into a directed graph. This graph shows each Bitcoin address as a node and the edges show the transaction between those addresses. One of the most important characteristics of this graph is that each transaction connects to the previous one by the "Previous Transaction Hash," the structure of which is temporal and changes over time, as it reflects the sequentiality of Bitcoin transactions is given in Figure 5.

Subsequently, Normalization is performed on transactional values, including the amount transferred and transaction fees using z-score standard scaling. This makes it possible to bring these features to an equivalent scale and make the machine learning models perform better than if one of the features dominates the others due to the differences in their values. Since Bitcoin transactions happen over time, Temporal Segmentation partitions the data into temporal segments. This makes it possible for the model to capture dynamics of the transaction network over time, to track the temporal characteristics of transaction behaviour over time which is crucial when looking for anomalies or fraud. Moreover, the transaction labels, which denote if a transaction is illicit or legitimate, undergo a process known as Label Encoding. These labels are converted into binary format to ease the classification process during the training of the binary classifiers in machine learning. Lastly, due to the managing of the large amount of data efficiently, the Graph Sampling methods are employed to form smaller subgraphs from the transaction graph. This helps to reduce the computational load during model training but at the same time, enables the model to learn from the large graph without overwhelming it with the entire dataset.

## 3.4 Model Development: GTAD (Graph-based Transaction Anomaly Detection)

The GTAD (Graph-based Transaction Anomaly Detection) model is designed & implemented for identifying transaction abnormalities in the Bitcoin. It uses GCNs and T-GCNNs to represent the temporal graph of Bitcoin transactions and transformers to detect anomalies. The main strength of the presented GTAD model is flexibility in detecting different kinds of anomalies in the transaction network, as well as spatial and temporal dependencies. The spatial dependencies are defined with regards to the links of the transactions in the transaction graph and temporal dependencies are defined with regards to the changes in these links with time. In the GTAD model, both of these types of dependencies help to detect relatively complex and high-level fraud schemes that are not easily recognizable.

### 3.4.1 Graph Convolutional Networks (GCNs)

The first primary component of the GTAD model is the Graph Convolutional Networks (GCNs) that describe the spatial dependencies of Bitcoin transactions as shown in Figure 5. GCNs are types of neural networks that work on the graph data and each transaction can be considered as a node and the connection between these transactions (Bitcoin flow from one transaction to another) as edges. GCNs function in a way that they take information from all the neighbors of a node in the graph and then extract the underlying patterns and dependencies in the transaction network from the model. This capability is very useful for identifying unusual transactions that are different from typical patterns of transactions, for example, groups of transactions or trends of transactions that are different from the normal

flow. Thus, GCNs can detect irregularities in the structure of the Bitcoin transaction graph that may suggest fraudulent actions or criminal transactions, which can be considered a significant advantage over other, purely statistical methods of anomaly detection, which do not take into account spatial relations between transactions.

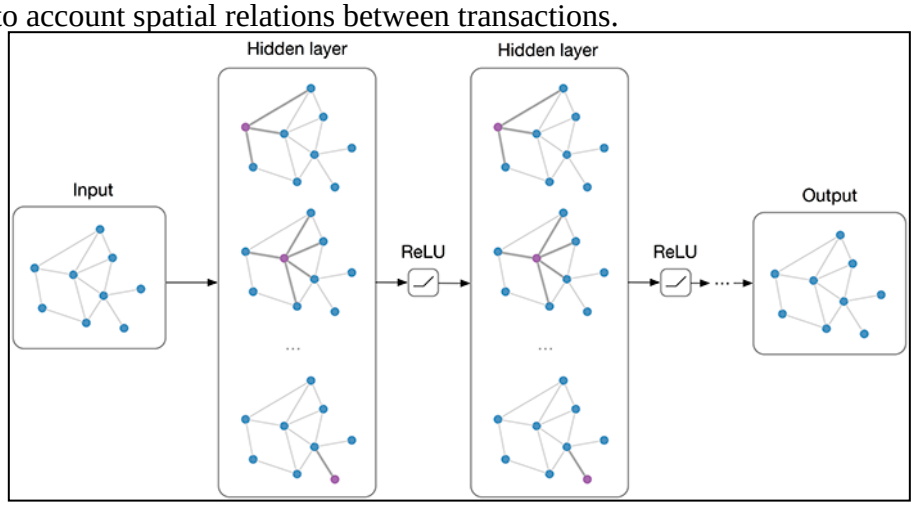



**Figure 5: Architecture of Graph Convolutional Networks**

### 3.4.2 Temporal Graph Convolutional Networks (T-GCNs)

To enhance the capability of the model in capturing anomaly patterns, GTAD integrates Temporal Graph Convolutional Networks (T-GCNs), which are improvements of the earlier GCNs based approaches with additional temporal domain of Bitcoin transactions. T-GCNs are also required to capture temporal dependency in the transaction patterns that might evolve over time. Certain types of frauds, for instance, money laundering or pyramid schemes may appear in the course of time and, therefore, it is rather difficult to distinguish them with the help of the transaction graph at a given moment. T-GCNs meet this challenge through the preprocessing where transaction data is segmented based on time. These time-based segments are then fed into the T-GCN layers to learn how the connection between transactions changes. This temporal analysis assists GTAD models to identify the gradual emergence of suspicious activities, the abrupt change of the transaction patterns that may reveal slowing down the fraud or money-laundering process.

### 3.4.3 Transformer Layers

In addition to GCNs and T-GCNs, the GTAD model utilizes Transformer layers, which are renowned for capturing long-range dependency in sequential data. Self-attention allows the model to modulate the input parts based on other parts, and in the case of Transformers, the model pays attention to the significant nodes and edges in the transaction graph of inputs. Self-attention enables the model to capture long-range relationships between the nodes within the graph which are useful when dealing with complex fraud schemes which might not be related to other fraudulent members. For instance, a fraudulent scheme can be a series of transactions that are scattered in different regions of the network, but the Transformer layers let the model link these transactions, even though there is no direct connection between them in the graph. This inherent ability of looking at long-range dependencies helps enhance the model's performance in identifying the complex fraudulent patterns that cannot be evaluated independently of the entire transaction network.

In conclusion, GTAD model employs an efficient approach to provide a effective solution for identifying the anomalies of Illicit Bitcoin transactions. For this purpose, the model uses Graph Convolutional Networks (GCNs) for spatial analysis, Temporal Graph Convolutional

Networks (T-GCNs) for temporal analysis, and Transformer layers with hierarchical attention mechanisms to capture local and global features in the transaction graph and changes in these features over time. The combination of spatial, temporal, and attention strategies makes GTAD best suited to identify singular and multiple fraudulent transactions, simple and complex frauds, simultaneously improving efficiency and reducing the amount of data analyzed to the most relevant portion of the transaction network. The integration of the GTAD model helps in detecting different fraud schemes and other suspicious activities in the Bitcoin transactions and can be regarded as a more efficient improvement compared to the conventional methods to anomaly detection in the cryptocurrency networks.

## 3.5 Model Training and Evaluation

### 3.5.1 Model Training

The GTAD model is trained using supervised training approach since the dataset is pre-labeled to differentiate between the licit and illicit Bitcoin transactions. The training process is initiated with the help of a **binary cross-entropy loss function** which determines the deviation of the identified labels of transactions from the actual labels. This loss function is especially used when the output is a binary decision, for instance, one between fraudulent and normal transactions. To enhance the performance of this model, the **Adam optimizer**, which is a stochastic gradient descent, is used to minimize the loss function. The hyperparameters such as the learning rate are further tuned with the help of the **grid search** algorithm in order to select the best hyperparameters that enhance the performance of the model.

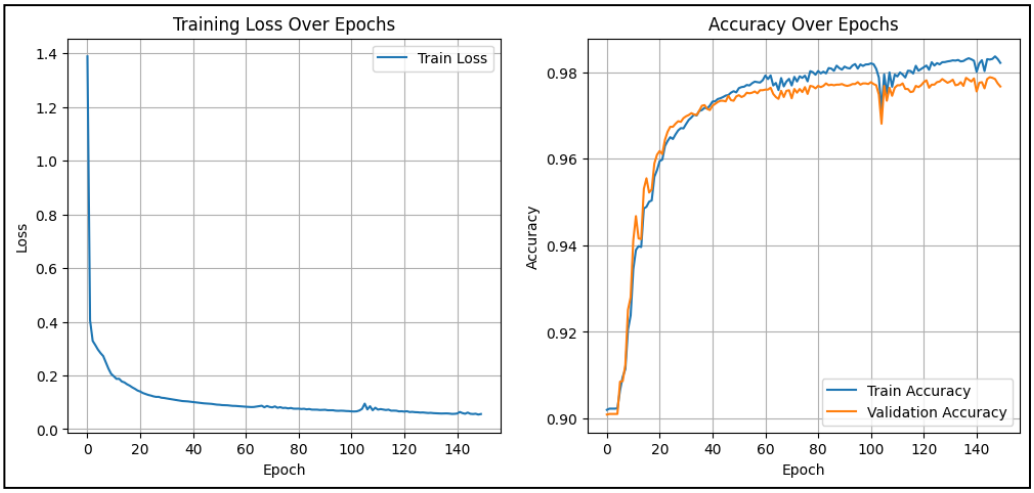



**Figure 1: GTAD Model Training Loss & Accuracy Over (150 Epochs)**

As for the training configuration, the dataset is divided into 70% training set, 15% validation set and 15% testing set. The model is trained in a batch size of 128 for 150 epochs. For proposed model, experimented with various learning rates of values 0.1,0.01,0.001 and 0.0001 and observed 0.01 provided better convergence using Adam optimizer and a weight decay of 0.0005. The model was trained for 150 epochs because this was sufficient for convergence, where the training and validation losses stopped improving, avoiding overfitting. The batch size of 128 was selected based on available system resources and provided an effective balance between training speed and memory usage. Dropout helps in overfitting since neurons are randomly removed, improving generalization. These settings make GTAD to be properly trained, and therefore capable of detecting the presence of anomalous transactions in unseen data.

### 3.5.2 Evaluation Metrics

The performance of the GTAD model is evaluated using several standard metrics for classification tasks:

**Table 2: Evaluation Metrics**

| No. | Metrics | Description |
|---|---|---|
| 1 | Accuracy | Accuracy metrics which measures the overall correctness of the model's predictions by calculating the proportion of correctly classified transactions. |
| 2 | Precision | The ratio of true positive predictions (illicit transactions correctly identified) to all positive predictions, providing insight into the model's ability to avoid false positives. |
| 3 | Recall | The ratio of true positive predictions to all actual positives, indicating the model's ability to detect all illicit transactions. |
| 4 | F1-Score | The harmonic mean of precision and recall, used to balance both metrics and provide a single performance measure. |
| 5 | AUC-ROC | This metric evaluates the model's ability to distinguish between positive (illicit) and negative (legitimate) transactions across various thresholds. A higher AUC-ROC indicates better model performance. |

## 3.6 Baseline Models and Comparative Experimentation

To compare the performance of the GTAD model, several baseline models are considered which are Logistic Regression, Random Forest, and the Decision Tree. Logistic Regression is a basic statistical model applied in binary classification problems, which makes it useful in identifying legitimate and fraudulent Bitcoin transactions. Logistic Regression is easy to use and easy to interpret but it fails to learn complex patterns in graph-structured data, such as the one in a network of Bitcoin transactions.

The Random Forest model is a type of ensemble learning and is more effective in modeling than Logistic Regression in terms of non-linearity. It uses multiple decision trees whereby each tree is learned on different sample data set that has been randomly selected from the entire data set, and the output of the different trees is combined in order to come up with the final decision. Nevertheless, Random Forests also have issues with temporal or relational dependencies inherent in the Bitcoin transaction data, so it cannot track new patterns over time. Also, a Decision Tree is employed as another basic model to be tested independently. Decision Trees are one of the simplest and powerful techniques of data partitioning which uses the feature values to construct a tree like structure to make decisions. Despite being simple to use and interpret, using Decision Trees for Bitcoin transactions analysis can lead to overfitting since there are many features and many interconnections between them.

For the Random Forest model, the 5-fold cross-validation with grid search focused on the number of estimators, tuning values such as 5, 10, 20, 100, and 500. Additionally, other hyperparameters like the minimum samples required for a split (min_samples_split), the minimum samples required for a leaf node (min_samples_leaf), the maximum depth (max_depth), and the method for selecting features (max_features) were tuned to optimise the model's performance. For the Decision Tree model, the grid search tuned the minimum samples required for a split (min_samples_split), exploring values like 2, 5, and 10, along with the minimum samples required for a leaf node (min_samples_leaf), the maximum depth (max_depth), and the criterion for measuring the quality of a split (criterion). For baseline Logistic Regression (LR) model, the grid search with various hyperparameters of maximum number of iterations (max_iter), tuning values such as 10, 100, 1000, and 10000, while also regularisation strength (C), and the solver (solver) tuned for optimisation.

All three models, Logistic Regression, Random Forest, and Decision Tree, use the same data set and performance metrics as the GTAD model. This brings a level of consistency with which GTAD's more sophisticated methods like GCNs and Transformer layers are better placed at detecting anomalies. By means of this comparative experimentation, it is demonstrated that the GTAD model is more capable of recognizing both spatial and temporal dependencies existing within the transaction network as compared to the traditional models, thereby making it a better solution to detect anomalies and fraudulent activities in Bitcoin transaction domain.

## 3.7 Summary

In this section, the specific procedure applied in the GTAD model was described in detail. It is a process of collecting and preprocessing data and then building, training and testing the model, which can be considered as a step by step approach towards detecting fraudulent Bitcoin transactions. Such techniques as GCNs, T-GCNs, and the transformer layers are included in the proposed model, and they form a novel approach to the anomalous detection in the cryptocurrency networks. In conclusion, the evaluation methods and comparative models ensure the efficiency of the model and the reliability of the GTAD model, and the model interpretability methods provide information on the decision-making of the model.

# 4 Experimental Model Results and Discussion

In this section, present the detailed evaluation of the proposed GTAD (Graph-based Transaction Anomaly Detection) model and compare it with the baseline models such as Logistic Regression, Decision Trees, and Random Forests. The performance of each model is evaluated using more than one measure including accuracy, precision, recall, F1-measure, and AUC-ROC. These metrics give overall idea of how each model works to identify the fraudulent Bitcoin transactions in nature of dataset which is highly imbalanced and complex in relationships among the transactions.

**Table 3: Evaluation Metrics for Baseline Models and GTAD Model**

| Model | Precision (Class 1) | Recall (Class 1) | F1-Score (Class 1) | Accuracy | Macro Average | Weighted Average |
|---|---|---|---|---|---|---|
| **Logistic Regression** | 0.99 | 0.84 | 0.91 | 0.85 | Precision: 0.69, Recall: 0.89, F1: 0.73 | Precision: 0.93, Recall: 0.85, F1: 0.88 |
| **Decision Tree** | 0.93 | 0.96 | 0.95 | 0.90 | Precision: 0.72, Recall: 0.66, F1: 0.69 | Precision: 0.89, Recall: 0.90, F1: 0.89 |
| **Random Forest** | 0.96 | 1.00 | 0.98 | 0.96 | Precision: 0.98, Recall: 0.82, F1: 0.88 | Precision: 0.97, Recall: 0.96, F1: 0.96 |
| **GTAD Model** | **0.98** | **0.99** | **0.99** | **0.98** | **Precision: 0.95, Recall: 0.92, F1: 0.94** | **Precision: 0.98, Recall: 0.98, F1: 0.98** |

## 4.1 Evaluation on Test Set for Baseline Models

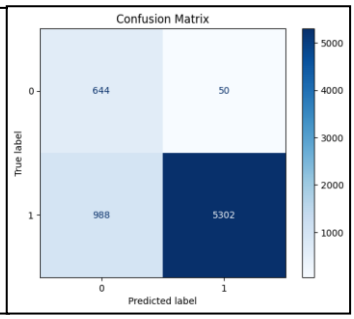
### Logistic Regression

On the test set the Logistic Regression model attains an accuracy of 85 per cent. However, the results for class "1," which represents illicit transactions, illustrated that the method had a

lower recall rate than the precision one. In particular, the model was 0.99 precise and 0.84 recall for illicit transactions. This means that while the model's precision is high, meaning that when it classifies a transaction as illicit, it is usually right most of the time, the model misses a large number of illicit transactions compared to when it identifies them (as observed by the low recall). A high value of precision and a comparatively low value of recall indicate that the Logistic Regression model is quite selective in detecting the illicit transactions and may actually miss out on a majority of them while at the same time, providing very few false alarms.

Classification Report:

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| 0 | 0.39 | 0.93 | 0.55 | 694 |
| 1 | 0.99 | 0.84 | 0.91 | 6290 |
| accuracy | | | 0.85 | 6984 |
| macro avg | 0.69 | 0.89 | 0.73 | 6984 |
| weighted avg | 0.93 | 0.85 | 0.88 | 6984 |



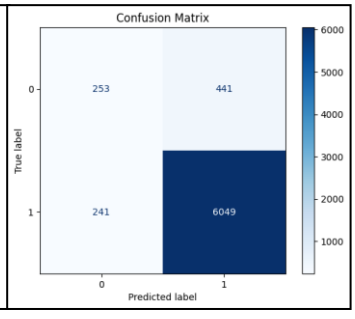

This problem is also evident in the confusion matrix for Logistic Regression where the model correctly classified 644 legitimate transactions (TN) and 5302 illicit transactions (TP) but at the same time; it misclassified 50 illicit transactions as legitimate (FP) and 988 legitimate transactions as illicit (FN). This indicates that the model tends to miss out on some misclassifications of illicit transactions out rightly in an imbalanced dataset where most of the transactions are legal.

**Decision Tree**

The Decision Tree model performed better than the Logistic Regression with the test set accuracy of 90%. It had an precision of 0.93% and a recall of 0.96% for the illicit transaction. This means that, the Decision Tree model had a better capacity of identifying cases of illicit transactions than the Logistic Regression model; with more capacity of not missing out cases (as depicted by the greater recall of the model). The F1-score for illicit transactions was 0.95 that means it was equally effective at both recalling illicit transaction while controlling the number of false positives.

Classification Report:

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| 0 | 0.51 | 0.36 | 0.43 | 694 |
| 1 | 0.93 | 0.96 | 0.95 | 6290 |
| accuracy | | | 0.90 | 6984 |
| macro avg | 0.72 | 0.66 | 0.69 | 6984 |
| weighted avg | 0.89 | 0.90 | 0.89 | 6984 |



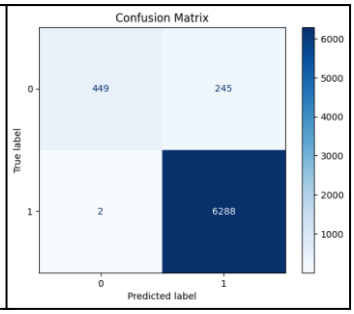

However, the difficulty was still present in the Decision Tree model as it contains false positives. The matrix of confusion shows that there were 441 false positives, which means that the model marked a large number of genuine transactions as fraudulent. The results showed that the model had reasonable precision and recall values, but there were false positives, which means that there would be too many investigations that were not necessary, thus compromising the efficiency of using such a model in the field.

**Random Forest**

Among the baseline models, Random Forest had the highest accuracy at 96%, and the highest Precision of 0.96, and Recall of 1.00 for illicit transactions. The high value of precision shows that when the model suggests an illicit transaction, it is probably true most of the times, while the value of recall is very high, meaning that most of the illicit transactions will be recognized by the model. However, the main problem of Random Forest, as noted in the results, is the high number of false positives, with 253 false positives in the confusion matrix. This is rather problematic in fraud detection as it implies that the model endorses a myriad of genuine transactions as fraudulent.

Classification Report:

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| 0 | 1.00 | 0.65 | 0.78 | 694 |
| 1 | 0.96 | 1.00 | 0.98 | 6290 |
| accuracy | | | 0.96 | 6984 |
| macro avg | 0.98 | 0.82 | 0.88 | 6984 |
| weighted avg | 0.97 | 0.96 | 0.96 | 6984 |




Thus, the obtained results have relatively high overall accuracy, but low macro-average recall, which equals 0.82. The model performs poorly with legitimate transactions because of the dataset's imbalance. From the results presented above it can be concluded that Random Forest model tend to overfit more to the majority class, thus less focus is given to the minority class of illicit transactions. Therefore, as while it has good accuracy in identifying the illicit transactions, high false positive rate and low recall value of the legitimate transactions make it less useful in identifying the Bitcoin transaction frauds.

## 4.2 Training of the GTAD Model

The GTAD model was trained using a graph-based deep learning approach to capture the relationship and patterns of Bitcoin transactions. In this case, training and validation accuracy increased gradually through 150 epochs of training. For the final epoch, the model has attained the training accuracy of 98.49% and the validation accuracy of 97.87% which will ensure the model will generalize well to unseen data. This strong performance indicates that the model is learning the latent features of illicit transactions from the training set and can generalize well to the validation set. The loss function, which calculates the difference between the predicted and actual labels, also reduced gradually with the epoch, showing the model is reducing the loss and improving the prediction. This consistent training behavior, along with high accuracy on both the training and validation set, proves the stability and effectiveness of the GTAD model.

**Table 4: History of Training Details of the GTAD Model**

| Epoch | Loss | Training Accuracy | Validation Accuracy |
|---|---|---|---|
| 10 | 0.2057 | 0.9238 | 0.9280 |
| 20 | 0.1438 | 0.9574 | 0.9609 |
| 30 | 0.1161 | 0.9670 | 0.9694 |
| 40 | 0.1022 | 0.9722 | 0.9712 |

| | | | |
|---|---|---|---|
| 50 | 0.0913 | 0.9753 | 0.9744 |
| 60 | 0.0839 | 0.9781 | 0.9758 |
| 70 | 0.0827 | 0.9784 | 0.9758 |
| 80 | 0.0761 | 0.9794 | 0.9762 |
| 90 | 0.0720 | 0.9805 | 0.9772 |
| 100 | 0.0671 | 0.9818 | 0.9772 |
| 110 | 0.0798 | 0.9794 | 0.9764 |
| 120 | 0.0666 | 0.9807 | 0.9769 |
| 130 | 0.0602 | 0.9825 | 0.9775 |
| 140 | 0.0571 | 0.9842 | 0.9792 |
| 150 | 0.0509 | 0.9849 | 0.9787 |

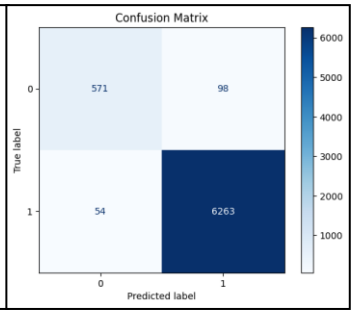
The GTAD model was trained using a graph-based deep learning model, where a clear increasing pattern in both training accuracy and validation accuracy were observed after 150 epochs. Table 4 illustrates that the training accuracy rose from 92.38% at epoch 10 to 98.49% at epoch 150, with validation accuracy rising from 92.80% to 97.87% during the same process. The loss function in training continued to reduce throughout the epochs, from 0.2057 at epoch 10 to 0.0509 at epoch 150, showing that the model reduced the errors. Such a trend indicates that the GTAD model was gradually learning the structure of the illicit transactions and was able to generalize well to new data instances. The high accuracy on the training and validating sets also confirms the model's stability and applicability to real-life fraud identification.

## 4.3 Evaluation of the GTAD Model

When the GTAD model was tested on the test set the results were better than baslines. The model proposed in this research study obtained an overall accuracy of 98.49% which is higher than the baseline models. For illicit transactions, the GTAD model yielded an accuracy level of 0.98, recall of 0.99, and an F1 score of 0.99. These metrics suggest that the GTAD model is very good at predicting the illicit transactions and also at capturing nearly all the predicted illicit transactions. This is a strength of the GTAD model as it reduces both FP and FN hence the reliability of the model in identifying fraudulent transactions.

Classification Report:

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| 0 | 0.91 | 0.85 | 0.88 | 669 |
| 1 | 0.98 | 0.99 | 0.99 | 6317 |
| accuracy | | | 0.98 | 6986 |
| macro avg | 0.95 | 0.92 | 0.94 | 6986 |
| weighted avg | 0.98 | 0.98 | 0.98 | 6986 |




The GTAD's confusion matrix states that the model successfully detected 6263 illicit transactions and 571 legal transactions, while the false positive was 98 and the false negative 54. This shows that the proposed GTAD model is very accurate in the identification of the legal and the illegal transaction, with little misclassification. Since the model can identify illicit transactions with very low rates of false positives, it would be effective in a real-world fraud-detection setting where minimizing false alarms is important for system efficiency.

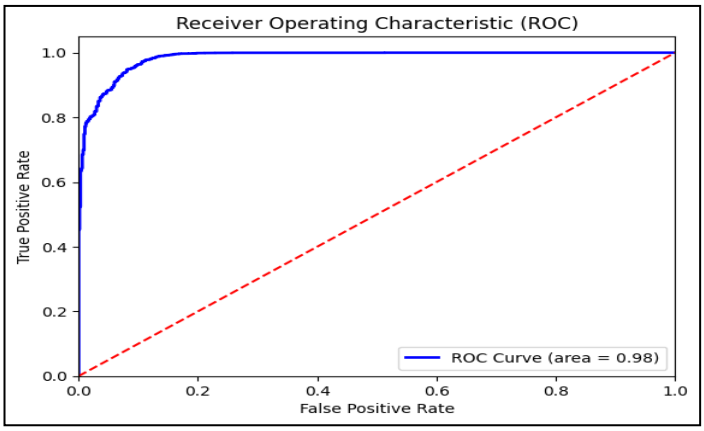



**Figure 2: ROC AUC Curve for GTAD Model**

Also, the AUC-ROC of 0.98 shows how well the GTAD model is capable of differentiating between the illicit and legitimate transactions in different decision thresholds. The value of AUC is high therefore the model is very efficient in its ability to classify data sets between the two classes regardless of the nature of the tests made. All of this contributes to the further strengthening of the model and its performance in general.

## 4.4 Discussion

From result it is evident that proposed GTAD model able to achieve 98.49% accuracy compared to baseline models like Logistic Regression, Decision Trees, and Random Forests with results of 85%, 90% and 96% respectively as reported in Table 3. The GTAD model outperforms the baseline models because it is designed to capture spatial and temporal dependencies between transactions using Graph Convolutional Networks (GCNs), Temporal Graph Convolutional Networks (T-GCNs), and Transformer layers.

The grid search was performed, with hyper parameter tuning performed and it helped to improve results of decision tree and random forest with 5-fold cross-validation with grid search. The results from the k-fold cross-validation with grid search optimization demonstrate more consistent performance over all metrics across all folds.

The results of the baseline models show that there is a significant difference in the ability of the models to detect the illicit transactions. Logistic Regression model had an accuracy of 85%, the precision of 0.99 and recall of 0.84 for the illicit transactions. Although it demonstrated promising performance by precisely detecting all the flagged illicit transactions, the relatively low recall values implied that it failed to point out a large number of such cases, which is obviously a major drawback in fraud detection. The F1-score of the model was 0.91 that showed the conflict of interests between precision and recall. The Decision Tree model was better still with an average accuracy of 90%, a precision of 0.93 and recall of 0.96 for the illicit transactions. The F1-score was higher with 0.95 which means better detection rate of illicit transactions but still it gave false positives 441 which can be costly in real world usage. Another important feature is that Random Forest model had the highest accuracy of 96%, the precision of 0.96 and the recall of 1.00 for the illicit transactions which shows high efficiency in detecting illicit transaction. However, it reported 245 false positives and was unable to distinguish between genuine transactions and fraudulent ones as evidenced by a macro-average recall of only 0.66 which indicates overfitting to the majority class.

**GTAD Model's Superior Performance:**
However, the result of the proposed GTAD model was significantly better than the baseline models. Due to its ability to apply attention mechanisms to concentrate on the relevant elements of the transaction graph, the architecture of the GTAD model allows for the detection of illicit activity patterns. This leads to the creation of a model which is highly accurate and highly sensitive, hence, few false positives and less false negatives. The GTAD model had a high accuracy of 98.47%, precision of 0.98, recall of 0.99, and F1-score of 0.99 for illicit transactions. The confusion matrix for GTAD also illustrates the model's performance, as it accurately finds 6263 illicit transactions and 571 legitimate transactions with 98 false positives and 54 false negatives. This demonstrates that the GTAD model was able to capture most of the illcit type of bitcoin transactions while excluding the licit ones with a high level of accuracy. Further, the AUC-ROC of the proposed model was 0.98, which ensures that the model can identify the illicit transaction from the legal one even if the dataset was imbalanced. The high AUC score also confirms that the model is very good in different decision thresholds, which is highly desirable in the real-world fraud detection system where false positive is very costly while at the same time high detection rate is crucial.

### Conclusion
Thus, the proposed GTAD model helps moving forward to identify Bitcoin transaction anomalies from the baseline models. The results have revealed the high value of the percentage of accuracy of 98.49%, precision of 0.98, recall of 0.99 F1-score of 0.99 and AUC-ROC of 0.98 proving that it can actually catch the bad transactions and reduce false positives. As a result, GTAD is more prepared to analyze transaction graphs and temporal dependence, which is crucial in identifying high-level fraud in Bitcoin networks compared to baseline models. The GTAD model is, therefore, a promising solution for the improvement of the security and trustworthiness of the Bitcoin transactions and could be further expanded to other cryptocurrency or financial transaction anomaly detection applications making the model highly versatile and useful in the other fields of the financial fraud detection domain.

# 5 Conclusion and Future Work

## 5.1 Conclusion
In this study, the performance of the ML models such as Logistic Regression, Decision Tree, Random Forest, and the developed GTAD model is assessed to detect the illicit activities related to Bitcoin transactions. In the same way, we conducted an experiment using the real-world dataset to show the performance of these models in identifying the fraudulent transactions and the strength and limitations of each model. The performance of the GTAD model was higher than the baseline models in each of the evaluation criteria used in this study. Obtaining the satisfactory results, including accuracy of 98.49%, precision of 0.98 and recall of 0.99, the GTAD model confirmed its high efficiency in the identification of the illicit transactions in cryptocurrencies environment. These results show that the model can be a valuable asset for regulatory authorities, financial organizations, and cybersecurity professionals who aim to prevent fraudulent actions and illicit activities within the cryptocurrency environment. However, Logistic Regression, Decision Tree, and Random Forest, being the baseline models, are somewhat restricted in their functionality. Comparatively, Logistic Regression and Decision Tree models exhibited low recall scores for the minority class (illicit transactions) signifying the difficulty in identifying fraudulent activities. Conversely, in the Random Forest model, it achieved a high recall for the class of

illicit transactions and low precision for the non-illicit class, which means a high likelihood of false positives. These results imply that, although the traditional models can be useful in fraud detection, they are less effective in dealing with the specifics of cryptocurrency transaction data as compared to the GTAD model. The training process of the GTAD model also demonstrated enhanced performance, where both training as well as the validation accuracy was above 150 epochs. The model's consistent convergence affirms its capability to prevent overfitting and thus, provides a sound solution for illicit transaction identification. Furthermore, the ROC-AUC score of 0.98 again supports the model in terms of discriminative capability of the model for illicit and non-illicit transactions.

## 5.2 Future Work

While the GTAD model shows promising results, there are several avenues for future work that could further enhance its performance and practical applicability. One potential direction is the incorporation of additional features, such as network-level information, user metadata, and behavioral analysis of Bitcoin addresses, which could improve detection capabilities, particularly for more sophisticated fraud schemes. Another important area of exploration is the real-time application and deployment of the model. Another major direction of further research is the practical use and implementation of the model in real time. While it is highly effective for static datasets, its implementation in real-time transactional environments introduces problems of scale, speed, and flexibility. Furthermore, transfer learning approaches could allow the model to be further trained for use on different cryptocurrency networks as well as various frauds including Ethereum or Litecoin. Since the type of cryptocurrency fraud is dynamic, it is also important to assess the model's adversarial robustness, to verify its accuracy in responding to adversarial strategies to deceive it. Last, engaging with the regulatory authorities to incorporate the GTAD model into other antifraud models could be helpful in developing a more extensive strategy for dealing with fraudulent actions in the cryptocurrency environment.

In conclusion, this study has shown that the GTAD model is a highly effective and sophisticated model for detecting illicit Bitcoin transactions, surpassing the traditional machine learning models.

# References

Alarab, I., & Prakoonwit, S. (2024). Robust recurrent graph convolutional network approach based sequential prediction of illicit transactions in cryptocurrencies. Multimedia Tools and Applications, 83(20), 58449-58464.

Bhatti, U. A., Tang, H., Wu, G., Marjan, S., & Hussain, A. (2023). Deep learning with graph convolutional networks: An overview and latest applications in computational intelligence. International Journal of Intelligent Systems, 2023(1), 8342104.

Ding, Z., Shi, J., Li, Q., & Cao, J. (2023). Effective Multi-Graph Neural Networks for Illicit Account Detection on Cryptocurrency Transaction Networks. arXiv preprint arXiv:2309.02460.

Fahmi, N., Hastasakti, D. E., Zaspiagi, D., Saputra, R. K., & Wijayanti, S. (2023). A comparison of blockchain application and security issues from Bitcoin to Cybersecurity. Blockchain Frontier Technology, 2(2), 58-65.

Huang, Z., Ren, Y., Pu, X., Huang, S., Xu, Z., & He, L. (2023, June). Self-supervised graph attention networks for deep weighted multi-view clustering. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 37, No. 7, pp. 7936-7943).

Lee, S., Kim, J., Seo, M., Na, S. H., Shin, S., & Kim, J. (2024). CENSor: Detecting Illicit Bitcoin Operation via GCN-based Hyperedge Classification. IEEE Access.

Mir, A. A., Zuhairi, M. F., & Musa, S. M. (2023). Graph Anomaly Detection with Graph Convolutional Networks. International Journal of Advanced Computer Science & Applications, 14(11).

Nie, L., Wang, X., Zhao, Q., Shang, Z., Feng, L., & Li, G. (2023). Digital twin for transportation big data: a reinforcement learning-based network traffic prediction approach. IEEE Transactions on Intelligent Transportation Systems, 25(1), 896-906.

Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2023, December). FraudLens: Graph Structural Learning for Bitcoin Illicit Activity Identification. In Proceedings of the 39th Annual Computer Security Applications Conference (pp. 324-336).

Nerurkar, P. (2023). Illegal activity detection on bitcoin transaction using deep learning. Soft Computing, 27(9), 5503-5520.

Olsson, A., & Andersson, D. (2024). The Dark Flows of Cryptocurrency: an overview of money flow behaviors in Bitcoin transactions related to online criminal activities and Bitcoin mixers.

Valem, L. P., Pedronette, D. C. G., & Latecki, L. J. (2023). Graph Convolutional Networks based on manifold learning for semi-supervised image classification. Computer Vision and Image Understanding, 227, 103618.

Shah, A. S., Karabulut, M. A., Akhter, A. S., Mustari, N., Pathan, A. S. K., Rabie, K. M., & Shongwe, T. (2023). On the vital aspects and characteristics of cryptocurrency—A survey. Ieee Access, 11, 9451-9468.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., ... & Polosukhin, I. (2017). Attention is all you need. Advances in Neural Information Processing Systems (NeurIPS), 30, 5998-6008. https://doi.org/10.48550/arXiv.1706.03762

Weber, M., Domeniconi, G., Chen, J., Weidele, D. K. I., Bellei, C., Robinson, T., & Leiserson, C. E. (2019, August). *Anti-money laundering in Bitcoin: Experimenting with graph convolutional networks for financial forensics*. KDD '19 Workshop on Anomaly Detection in Finance, Anchorage, AK, USA.