SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

Blockchain-Powered Deep Learning Model For Automated Bitcoin Entity Deanonymization And Forensic Analysis Of Transactions

ArjunBalaji B[1] , Dr.P.Velmurugadass[2]

[1]Research Scholar, kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India – 626126. Email id: arjundev492@gmail.com
[2]Associate professor, kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India – 626126.Email id: p.velmurugadass@klu.ac.in
Corresponding author mail id: arjundev492@gmail.com

Abstract
The pseudonymous design of the Bitcoin blockchain provides privacy to users but simultaneously enables illicit financial activities such as cybercrime, ransomware payments, and money laundering. This research proposes an advanced deep learning–driven framework for blockchain entity deanonymization and behavioural classification, aimed at strengthening transparency, security, and regulatory compliance. The primary purpose of blockchain in this research is twofold: first, as the immutable and distributed data source for large-scale transaction analytics, and second, as a trusted ledger for recording and auditing AI-driven classification outcomes. Building upon foundational machine learning approaches, the proposed system employs Elephant Swarm Water Search (ESWS) for optimizing tuned hyperparameters-tuned Attention-based Graph Neural Networks (Att-GNN) for a graph learning model for entity deanonymization, and to capture complex structural, temporal, and transactional dependencies among Bitcoin addresses and clusters. A labelled Bitcoin Entity Transaction containing 2,870 records has been collected from Kaggle. It trains supervised deep learning models to classify unknown entities, enabling automated representation learning directly from transaction graphs, eliminating reliance on handcrafted features. To enhance accountability, model predictions, confidence scores, and decision logs are stored on a private blockchain, ensuring tamper-proof audit trails for regulatory and compliance purposes. Experimental evaluations demonstrate significant improvements in classification accuracy 98.45%, precision 96.0%, recall 92.0%, F1-score 95.0%, and MCC 97.0%. This research contributes a secure and intelligent blockchain analytics solution that integrates deep learning with decentralized ledger technology to support automated risk assessment and forensic investigations. The ESWS-Att-GNN framework provides entity deanonymization and classification to enhance forensic analysis and auditability.

Keywords: Illicit Activities, Bitcoin Transaction, Auditability, Logging, Cryptocurrencies, Bitcoin entity, and deanonymization.

1. Introduction

The Bitcoin blockchain is pseudonymous, which the users have some privacy of financial transactions. Bitcoin does not involve the identity disclosure of users and this is a degree of anonymity that assures individuals that they are not committing any illicit activities [1]. It allows secure, which is a good alternative to the traditional banking systems [2]. Its openness, which is made possible through the blockchain in its immutable nature, provides that the records of all transactions are publicly accessible, and it has a beneficial effect of instilling a feeling of trust in the users. In addition to that, the technology is scalable, which means that it allows global financial inclusion without necessarily having to limit it to geographical limits or intermediaries [3].

The pseudonymous nature of the Bitcoin, however, poses a serious challenge especially when it comes to illegal practices. Although it provides privacy, it contributes unwillingly to cybercrime, money laundering, and ransomware payments [4]. The fact that the transactions are anonymous, makes it particularly difficult

to track and prevent illegal actions, which is a major obstacle to regulation and transparency in the cryptocurrency sector [5]. The rapid expansion of blockchain networks adds to the complexity of the analysis of the transactions and makes the detection of suspicious activity more challenging. The technologies allow automated categorizing Bitcoin entities, which offer a more efficient and scalable way of transaction forensics [6].

It has been difficult to balance between privacy and accountability, identify the presence of illicit activities, scale, and preservation of tamper-proof forensic records [7]. Was supposed to anonymize blockchain transactions by organizing them, differentiating between legitimate transactions and illegitimate ones [8]. Utilized ensemble learning algorithms, such as XGBoost, RF, and Bagging, to obtain an improved accuracy in a transaction classification. There were mixed results with varying information and poor model performance with unbalanced classes.

Identified money laundering clusters in Bitcoin through a contrastive learning method based on subgraphs [9]. It proposed Bit-CHetG, which applies heterogeneous subgraphs and GNN to detect groups. Bit-CHetG showed an increase in Micro F1 Score at least 5 percent better than current processes. The strategy is susceptible to noise, and it needs to be optimized further in the context of scalability. Bitcoin pseudonymous architecture allows illegal practices, where it is hard to establish malicious actors, and certain tools cannot handle complex transaction structures, in need of an automated, scalable, and reliable system to deanonymize and analyze entities.

To address these loopholes, this study primarily contributes a DL-based framework to use the ESWS-biased attention-based GNN to perform automated Bitcoin entity deanonymization, classification, and tamperproof auditing. The model can be used by financial institutions and cybersecurity people to monitor, classify, and trace suspicious Bitcoin transactions, which decrease anonymity and promote proactive risk management and compliance.

1.1 Key contribution of this research

- Research aims to develop an Att-GNN framework optimized with ESWS for automated Bitcoin entity deanonymization, classification, and auditable forensic analysis.
- The Bitcoin Entity Transaction was obtained through Kaggle and consists of 2,870 records, such as the volume ID, total number of inflow and outflow, average transferred value, and entity label.
- The study suggests an ESWS-Att-GNN that will be used to classify entities and perform behavioural analysis to enhance scalability and efficiency. Practically enables the detection of illicit Bitcoin activities efficiently, providing scalable, accurate, and auditable entity classification for improved blockchain forensic investigations.

The research is structured to systematically present the proposed blockchain-driven DL framework. Section 1 provides the introduction of this research, Section 2 covers literature review, Section 3 covers formula of the problems, Section 4 methods, Section 5 presents performance analysis, Section 6 discusses the existing limitations and implications of this research, and Section 7 concludes with contributions and future directions of this research.

2. Related works

The related works focus on detecting and classifying suspicious Bitcoin network activity, fraud, and deanonymization using ML, graph analysis, and network fingerprinting with scalability challenges. Designed to detect and classify networking types in Bitcoin using network fingerprinting and ML [10]. Network fingerprinting was implemented with supervised ML models to identify IP and Tor usage. CatBoost and RF detected false claims with 93% accuracy and 94% for I2P. The challenges in scalability and real-time detection under varying network conditions.

Suspicious Bitcoin network activity was detected by evaluating ML methods using transaction-derived [11]. LR, DT, RF, and XGBoost were compared in terms of tuning and rebalancing. Gradient boosting was the most successful in terms of predicting crucial features of address. The constraints can be associated with the issues of feature selection, the imbalance of data, and hyperparameter optimization.

Illegal behavior in cryptocurrency was spotted through dealing with sample imbalance and untagged challenges [12]. It used mutual information and self-supervised learning and combined it with the GCN method in order to achieve better F1-score than the traditional methods, which makes their detection better. It had a scaling limitation and the inability to handle a large-scale cryptocurrency transaction. Wrote an argument structure to make implicit assumptions clearer and to think more effectively about legal in the cryptocurrency deanonymization [13]. Used legal arguments and interrogatives to assess cryptocurrency deanonymization methods. Enhanced the disclosure of premises underpinning, which can be used in judicial analyses of deanonymization investigations. It needs to be adjusted to a variety of legal contexts, as well as implemented practically in various jurisdictions.

Graph embeddings were created to be efficient and perform the de-anonymization process of a graph based on neural networks [14]. It used the method of graph convolutional networks, neural tensor networks and optimized greedy algorithm of node matching in order to enhance the efficiency and performance of graph de-anonymization. The performance was diverse and with very noisy or incomplete data of the graph, it needed more refinement.

Detected frauds in the transactions of bitcoins through the application of ML techniques to the characteristics of the transactions [15]. Transaction data was detected through anomaly detection algorithms to detect fraud. Unsupervised methods are applied in detecting fraud, whereas supervised graph techniques are applied to highlight the importance of heterogeneity. This performance was dependent on quality and needs to be optimized to achieve large scale networks.

Increased entity anonymity on Bitcoin and enhanced detection of unlawful conduct through alleviation of severe class imbalance in transactions [16]. Tested and compared three GAN architectures in order to produce synthetic behaviours of entities in Bitcoin that can be resampled by minority classes. The quality of GANs relies on their cost of computation and a lack of diversity in real-data. GAN-based resampling was more accurate, precise, recalling higher, and F1-score, which is better than conventional methods of preprocessing.

2.1 Research gap

The network fingerprinting, fraud detection, and deanonymization methods based on the ML and GNN-driven approaches have achieved good results when analysed with the Bitcoin network and transactions [10-12]. Nevertheless, the issues with scalability, real-time detection, imbalance in datasets, feature selection, and the big-scale or noisy graphs of transactions persist [13]. Moreover, it is not yet possible to combine legal reasoning, heterogeneous network analysis and automated entity classification with the strength of auditability, and a gap exists on a scalable, end-to-end DL framework incorporating graph learning, behavioural classification, and tamper-proof logging to support full Bitcoin forensic analysis [14-15]. Trains GANs to create artificial behaviour of entities in Bitcoin through usages that address the problem of class imbalance and enhance the detection of illicit behaviour [16]. The gap points to scalability, real-time detection, data imbalance, feature selection, noisy graphs, and absence of integrated and auditable frameworks of Bitcoin forensics. The study addresses such limitations by proposing the ESWS-Att-GNN model that has scalable and accurate Bitcoin entity classification with automated learning and auditability of a graph through blockchains.

3. Problem Formulation

The deanonymization problem is defined as having a Bitcoin transaction graph, where nodes correspond to reports and edges describe transactions, and foretells the real-world entity type of each address or cluster. It assumes labelled data availability while considering privacy and ethical constraints to ensure responsible, accurate entity identification.

4. Methodology

The present research aims to develop a DL framework for automated Bitcoin entity deanonymization, classified transaction behaviours, and ensured tamper-proof logging for forensic and regulatory analysis. Figure 1 illustrates a forensic framework where a Bitcoin transaction dataset feeds into an ESWS-optimized Attention-GNN to perform automated deanonymization, validated through comprehensive performance metrics and multi-dimensional data visualizations.

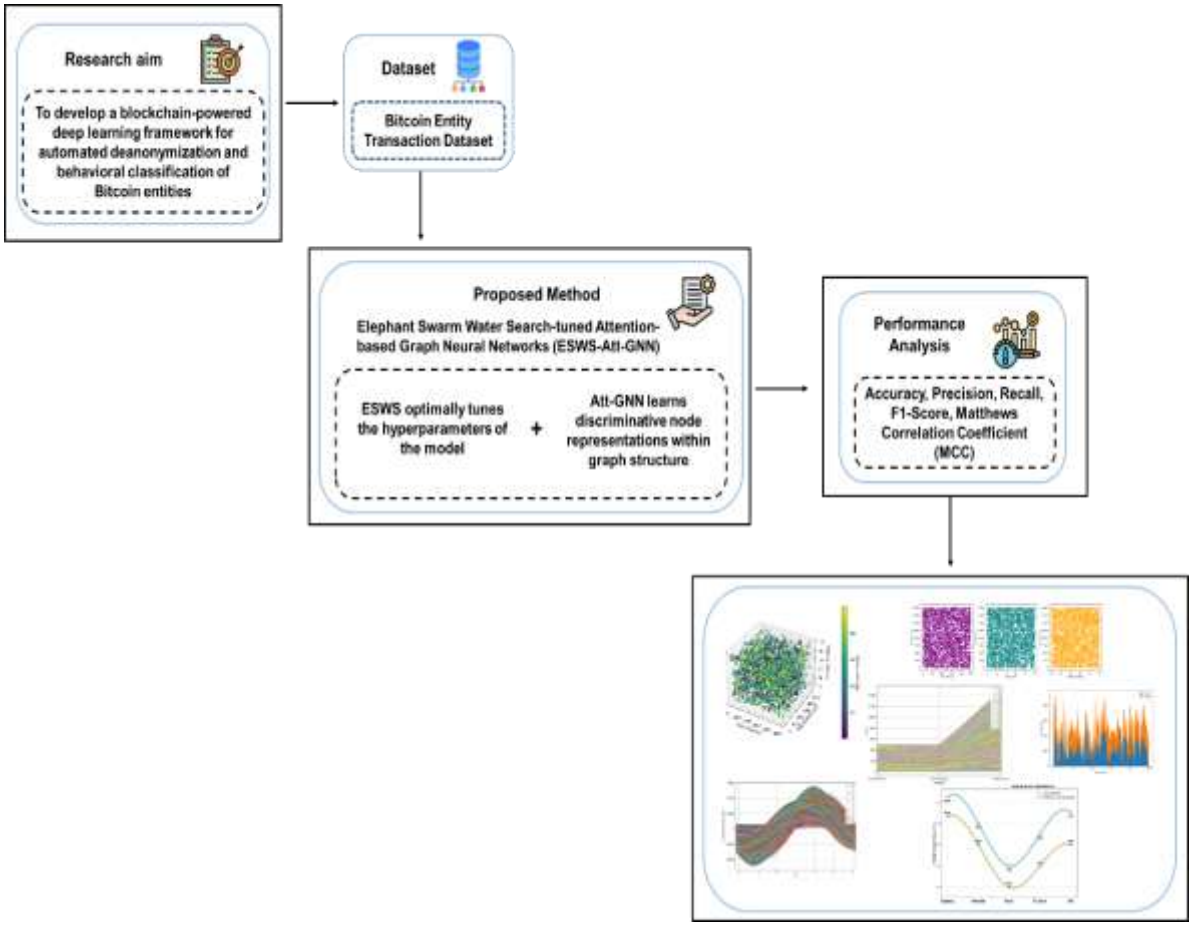

Figure 1: Architectural framework of the ESWS-Att-GNN model for automated Bitcoin entity deanonymization

4.1 Data collection

The Bitcoin Entity Transaction is utilized for this research, and it is collected from the open-source Kaggle platform. Data source link: https://www.kaggle.com/datasets/colabsss/bitcoin-entity-transaction-dataset. It contains 2,870 records collected from Bitcoin transaction activity representing entity-level profiles on the blockchain. It includes data on transaction volumes id, total inflow/outflow counts, average transferred value, temporal entropy, address count, transaction in and out value, active duration days, total incoming and outgoing ratio, and entity label.

4.2 Proposed Framework

The suggested structure employs an ESWS-Att-GNN to do automated deanonymization and forensic analysis of Bitcoin entities. The proposed approach combines Att-GNN which captures both the structural and temporal patterns in transaction graphs, producing latent node representations, and ESWS hyperparameters selection is done through the position-update functionality.

4.2.1 Attention-based Graph Neural Networks (Att-GNN)

The GNN bitcoin transaction graphs, capturing relationships between addresses, and learning latent patterns for effective entity deanonymization and classification. It processes Bitcoin transaction graphs, aggregates neighbouring address information, and updates features to identify patterns, enabling accurate entity classification for forensic analysis. Graph of Bitcoin addresses as nodes, transactions as edges, node features as transactions, optional edge features, adjacency matrix. The j-th layer of a GNN formulated in Equation (1):

$$g_j^s = \phi^1\left(g_j^{s-1}, \{g_i^{k-1}, \forall i \in M(j)\}\right), \quad (1)$$

The superscript k denotes the k--th layer, where g_j^{s-1} represents the feature representation of node j, and g_j^s is initialized as W_j , i is an index, and M is the number of neighbouring nodes. The aggregation function ϕ^1in Equation (2) facilitates inter-node information propagation and updates node feature representations

$$g_h = h\left(\{g_j^K, \forall j \in H\}\right) \quad (2)$$

The terminal node representation g_j^K after K iterations is a summary of all the nodes in the graph. In the case of graph-level tasks, global representation g_h is calculated by using an extra readout H with node embeddings.

Attention-Based GNN will help improve the ability of the model to prioritize the nodes and edges that are important in the Bitcoin transaction graph and thus increase the accuracy of the entity classification. It gives weight to the neighbors based on the dynamics of attentions so that the model focuses more on the important nodes and transactions, which maximizes the quality and speed of the entity deanonymization. The data that is fed in includes the Bitcoin transaction graph, the addresses, the relationships between transactions including the temporal dependencies to perform activities like entity deanonymization and behavioral classification. Here, aggregation ϕ in Equations (3) and (4) is an attention-based GNN. The attention-based aggregator at the j-th layer is formulated as follows:

$$f_{ji}^{k-1} = \mathrm{Att}\left(g_j^{k-1}, g_i^{k-1}\right), \quad (3)$$

$$\alpha_{ji}^{k-1} = \mathrm{softmax}\left(f_{ji}^{k-1}\right) = \frac{\exp\left(f_{ji}^{k-1}\right)}{\sum_{l\in\tilde{M}(j)} \exp(f_{ji}^{k-1})} \quad (4)$$

$$g_j^s = e^k\left(\sum_{i\in\tilde{M}(j)} \alpha_{j,i}^{k-1} g_i^{j-1}\right), \quad (5)$$

In Equation (5), f_{ji}^{k-1} denotes the attention coefficient, Att represents the attention function, and α_{ji}^{k-1} denote the attention weight, g_j^{k-1} is the attention coefficient from function Att, which quantifies the relationship between node i and node j, where g_i^{k-1} represents the attention weight computed using the softmax function. α is a neighboring node, $\exp\left(f_{ji}^{k-1}\right)$ represents exponentiation of larger values. $\sum_{i\in\tilde{M}(j)} \alpha_{j,i}^{k-1} g_i^{j-1}$ a normalization term summing exponentiated attention coefficients of all neighbors, $\tilde{M}(j)$ is a self-loop and e^k represent learnable transformation. Therefore, predicted entity types, confidence scores, and learned node embeddings for deanonymization and forensic analysis. Figure 2 visualizes the transformation of transaction graphs into entity classifications and robust precision across various categories, including exchanges and ransomware.

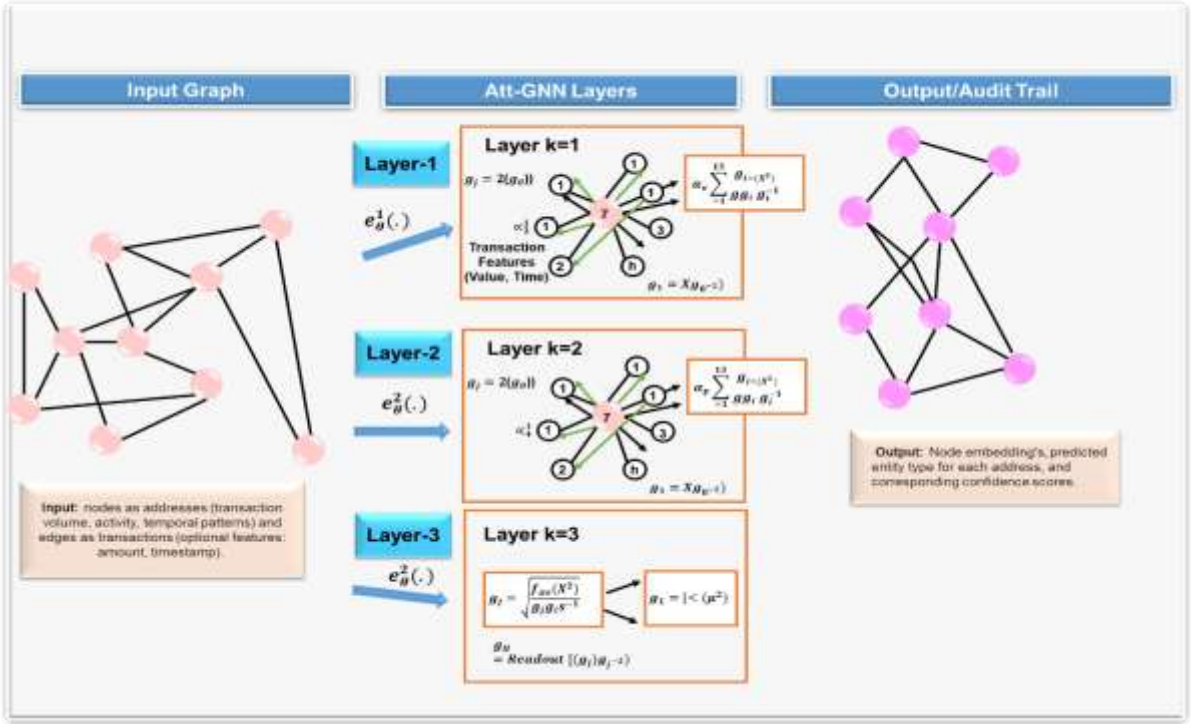

Figure 2: Att-GNN architecture across diverse Bitcoin entity classifications for automated forensic analysis

4.2.2 Elephant Swarm Water Search (ESWS)

The ESWS algorithm is applied to fine-tune the hyperparameters of the Att-GNN to improve the performance of the DL in classifying Bitcoin entities by refining attention weights. ESWS fine-tunes the attention coefficients between nodes, improving the model's ability to focus on more relevant transactions and addresses in Bitcoin transaction graphs, enhancing the accuracy of entity deanonymization. It includes hyperparameters such as learning rate, attention weights, and transaction graph. During droughts, elephants form groups known as elephant swarms and roam together in search of water, with each group

collaborating to find a water source. In Equation (6), exploration of both local and global regions is controlled by a probabilistic parameter called the switching probability o, where $o \in [0,1]$.

$$U_{j,c}^{s+1} = U_{j,c}^{s} x^{s} + qamd(1,c) \odot \left(H_{best,c}^{s} - W_{j,c}^{s}\right) \quad (6)$$

For a c-dimensional optimization problem, the position of the j-th elephant group in a swarm of W particles at iteration $s$is denoted by $W_{j,c}^{s}$, and its velocity is represented as $U_{j,c}^{s}$. The velocity at the next iteration, $U_{j,c}^{s+1}$ incorporates momentum from the previous step. The locally optimal solution for the j-th elephant group at the current iteration is expressed as $O_{\text{best},j,c}^{s}$, while the globally optimal solution is given by $H_{\text{best},c}^{s}$.

If $qand > O$ [for global search]

$$U_{j,c}^{s+1} = U_{j,c}^{s} x^{s} + qamd(1,c) \odot \left(O_{best,j,c}^{s} - W_{j,c}^{s}\right) \quad (7)$$

If $qand \leq O$ [for local search]

$$W_{j,c}^{s+1} = W_{j,c}^{s+1} + W_{j,c}^{s} \quad (8)$$

Equations (7) and (8), the position is updated according to the function $qand(1,c)$ generates random values, $\odot$ denotes element-wise multiplication, $W_{j,c}^{s+1}$ represent the updated position. x^{s} represents the inertia weight. ESWS optimized attention weights, refined node representations, and enhanced entity deanonymization accuracy and efficiency. Table 1 summarizes the key hyperparameters used in the ESWD-Att-GNN framework.

Table 1: Optimized Hyperparameters for the ESWS-Att-GNN Model

Hyperparameter	Symbol	Description	Optimized Value
Learning Rate	η	Controls gradient update magnitude during Att-GNN training	0.001
Number of GNN Layers	K	Depth of the Attention-based Graph Neural Network	3
Attention Head Size	H	Number of parallel attention mechanisms per layer	8
Dropout Rate	δ	Prevents overfitting by randomly deactivating neurons	0.5
ESWS Inertia Weight	x^{s}	Balances exploration and exploitation in ESWS search	0.7
Switching Probability	o	Probability controlling local vs. global water search	0.6

The parameters govern learning dynamics, network architecture, AM, regularization, and ESWM behaviour. The maintained values ensure stable convergence, effective representation learning in Bitcoin entity deanonymization and forensic classification. Algorithm 1 shows that ESWS-Att-GNN approach for bitcoin entity deanonymization and forensic transaction analysis.

Algorithm 1: Elephant Swarm Water Search- Attention-Based-Graphical Neural Network (ESWS-Att-GNN)

```
import numpy as np, random
softmax = lambda x: np.exp(x)/np.sum(np.exp(x))
relu = lambda x: np.maximum(0, x)
att = lambda h1, h2: np.dot(h1, h2)
def att_gnn(G, X, W):
  return {j: relu(W @ sum(softmax([att(X[j], X[i]) for i in G[j]])[k] * X[i]
      for k, i in enumerate(G[j]))) for j in G}
def fitness(params, G, X): return random.uniform(0.8,0.95)
def ESWS(G, X, T = 5):
  swarm = [{"p": {"lr": 0.01, "d": 8}, "v": {"lr": 0, "d": 0}, "best": 0} for _ in range(3)]
  gbest = {"score": 0}
  for _ in range(T):
    for e in swarm:
      s = fitness(e["p"], G, X)
```

```
        if s > e["best"]: e.update({"best": s, "bp": e["p"].copy()})
        if s > gbest["score"]: gbest.update({"score": s, "p": e["p"].copy()})
    for e in swarm:
        tgt = gbest["p"] if random.random() > 0.5 else e["bp"]
        for k in e["p"]: e["v"][k]
                = 0.5 * e["v"][k] + random.random() * (tgt[k] - e["p"][k]); e["p"][k]+= e["v"][k]
  return gbest["p"]
G = {0: [1,2],1: [0],2: [0]}
X = {i: np.random.rand(8) for i in G}
best = ESWS(G, X)
W = np.random.rand(best["d"], best["d"])
emb = att_gnn(G, X, W)
print("Optimized Params: ", best)
print("Node Embeddings: ", emb)
```

The integration applies optimized attention weights within the GNN aggregation mechanism, producing refined embeddings for accurate classification. The hybrid method ensures scalability, enhanced accuracy, and auditability. It applied Att-GNN to the graph learning and ESWS to optimize hyperparameters of tuning. The suggested ESWM-Att-GNN on hyperparameter optimization using an Attention-based GNN. It trains node embeddings using Bitcoin transaction graphs, generating optimal parameters to be used in the correct entity classification and forensic analysis.

4.2.3 Automated Entity Classification

Once the ESWS-Att-GNN is trained, the framework allows classifying newly unknown Bitcoin addresses and address clusters fully automatically. Using learned node embeddings, the model predicts the type of entity of exchange, merchants, mining pools, or illicit actors by deriving latent action between two parties. Additional aggregation Cluster-level embedding aggregation allows the identification of even higher-order organizational and network-wide patterns and makes it easier to detect coordinated, abnormal, or fraudulent activity. This end to end learning paradigm eliminates the need to combine both structural and time-based dependencies on the transaction graph to jointly learn the inherent address relationships in the transaction graph, and offers an intervention-free and scalable way to learn without manual feature engineering, a useful tool to discover hidden address relationships and achieve large-scale and intervention-free deanonymization in forensic blockchain analysis.

4.2.4 Blockchain Integrated Logging

To implement accountability and promote regulatory compliance, all outputs of the entity classifier, such as predicted label, confidence scores and metadata of decisions are permanently fixed to a personal blockchain. All the inferences are documented in a non-repudiable and tamper evidence ledger creating an audit trail that can be verified by post hoc analysis. Additionally, any intermediate artifacts that are critical, e.g. attention weight distributions and learned embedding states are continuously logged, so that forensic reconstruction of the decision logic of the model can be made and interpreted. The proposed framework will enhance transparency, reproducibility, and adversarial manipulation resistance by ensuring the tight integration of DL inference with blockchain immutability, thus strengthening trust and giving a solid infrastructure to risk assessment, governance, and compliance in decentralized financial systems.

4.2.5 Framework Overview

The overall methodology may be summed up as follows:

- Construct Bitcoin transaction graphs from blockchain data.
- Preprocess graphs to normalize features and encode temporal dynamics.
- Train ESWS-Att-GNN with optimized hyperparameters for entity classification.
- Classify unknown addresses and clusters automatically.
- Record predictions, confidence scores, and logs on a private blockchain for immutable auditability.

The context offers a precise, visible, and elucidable clarification of the blockchain forensic examination and promotes automatic evaluation of risks and regulatory standards.

5. Performance analysis

Successfully created a DL framework based on ESWS-Att-GNN and blockchain logging to automate entity deanonymization and forensics of transactions based on Bitcoin. Table 2 presents the hardware and software used as an experimental set up in this research. In this part, there are the visualisations of bitcoin transactions, behavioural clustering, entity deanonymization, temporal analysis, anomaly detection and blockchain-based forensic auditability.

Table 2: Hardware and Software setting in deanonymizing Bitcoin entities

Components	Specification
CPU	Intel Xeon Gold 6226R
RAM	128 GB DDR4
GPU	NVIDIA RTX 3090 24GB
Operating System	Ubuntu 22.04 LTS
Programming Language	Python
Libraries	PyTorch / PyTorch Geometric, NumPy / Pandas

5.1 Experimental analysis

The experimental outcome develops a DL framework integrating ESWS-Att-GNN and blockchain logging to automate Bitcoin entity deanonymization and forensic analysis. It presents visualizations, ESWS-Att-GNN performance, transaction patterns, behavioural clusters, deanonymization results, and blockchain-based forensic auditability.

Figure 3 gives a structural overview of ESWS-Att-GNN architecture and transaction graphs to make interpretation of high-dimensional data easier. It plots clusters of Bitcoin nodes in form of a visual node, with Attention layers indicated to illustrate suspicious transaction paths, and displaying the ESWS process of optimization. It gives a diagnostic picture of the deanonymized bodies in a clear manner and the efficiency of the model, where the investigators can trace the illicit financial flows in an intuitive way.

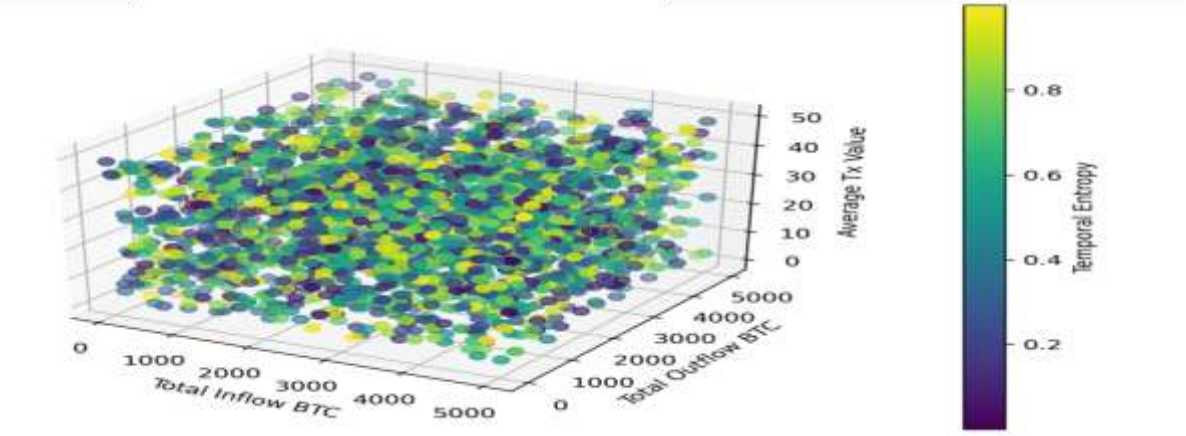

Figure 3: Multidimensional visualization of clusters of Bitcoin inflows and outflows indicating the total inflow, outflow, and average transaction of an entity to deanonymize

Figure 4 provides the interdependence of three important variables of transaction at the same time. It traces crude Bitcoin transaction streams across the attention-based neural network that is optimized via ESWS and documents final classifications to an unalterable ledger. A structural design that shows high-accuracy of deanonymization and probative auditability against regulation.

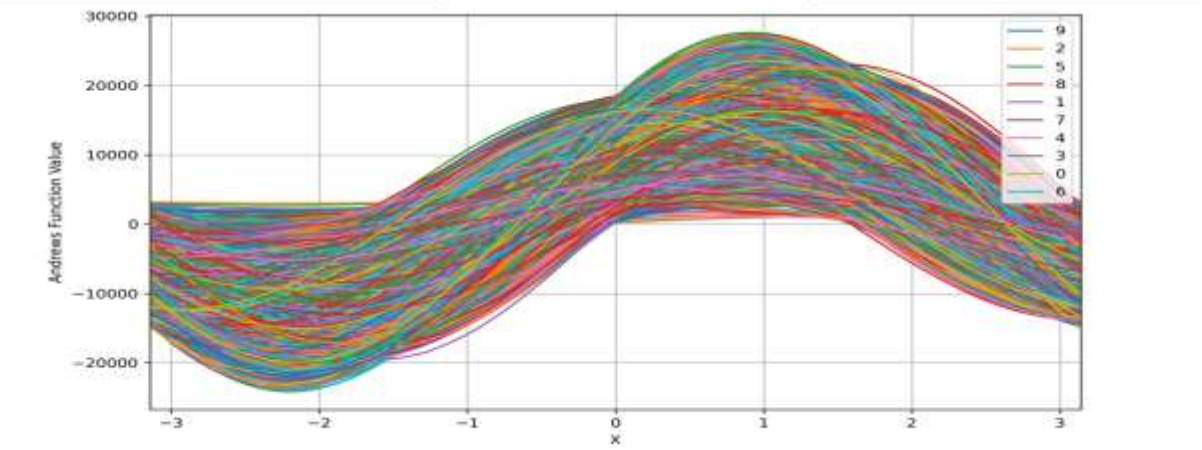

Figure 4: Visualization of Multidimensional Bitcoin Transaction Characteristics to Behavioural Clustering and Automated Entity Classification

Figure 5 visualizes transaction patterns of Bitcoin transactions in high dimensions, and detects behaviour clusters to deanonymize. It gives the inflow, outflow and entropy in the spatial models in order to show the anomalies. The visual clusters enable the distinction between the licit and the illicit agents to be identified, which allows quick identification of forensic risks.

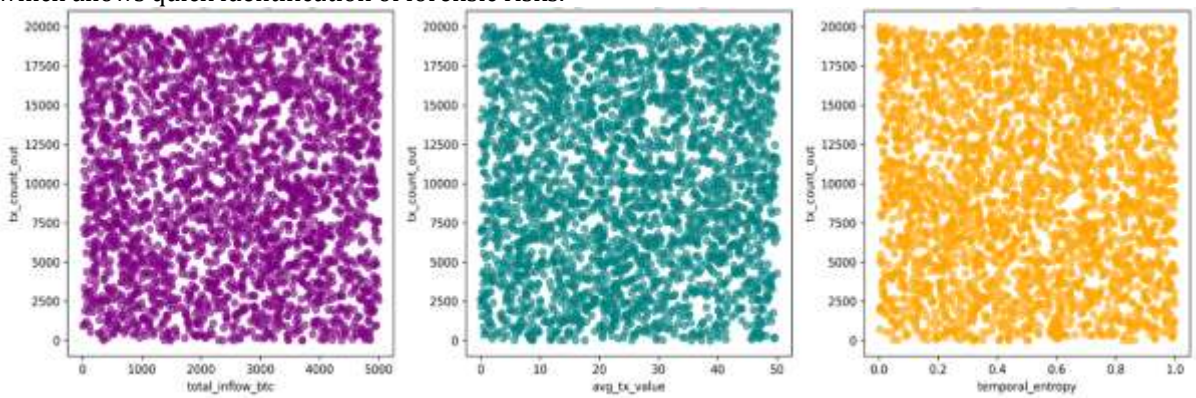

Figure 5: Distribution of number of transactions versus inflow, value and temporal entropy of Bitcoin entity behavioural analysis

Figure 6 is a tool to convert complex Bitcoin transaction data into visual patterns that are easy to read to perform entity deanonymization and classification of behaviour. The Parallel Coordinate Plots convert the multi variable entity features into the spatial pattern or continuous curve in order to detect the similarities. Visual clusters differentiate normal user behavior from illicit ransomware patterns, facilitating intuitive forensic discovery and risk validation.

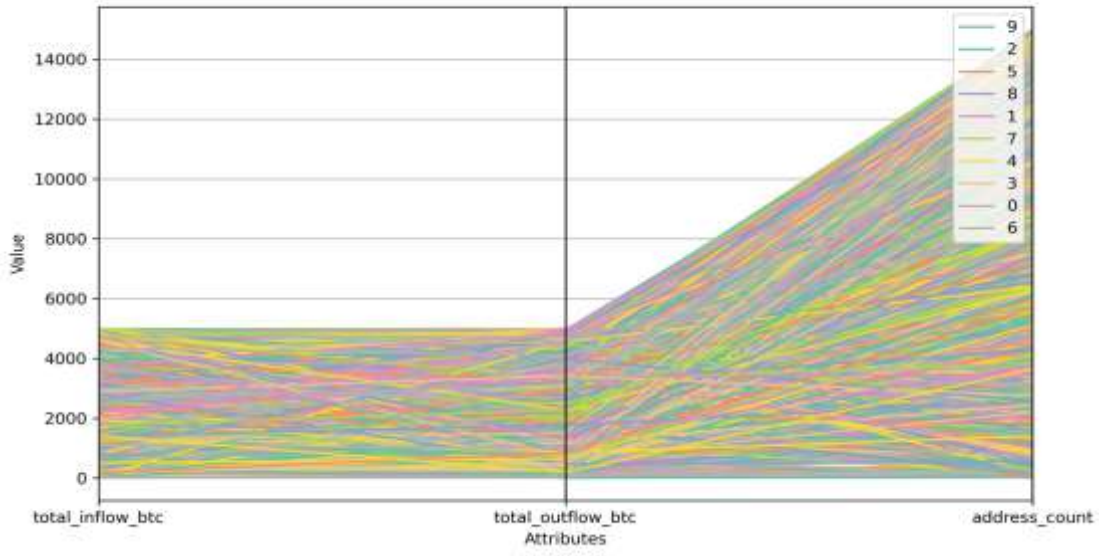

Figure 6: Parallel coordinate diagram of the distribution of total inflow, outflow and number of addresses within various clusters of Bitcoin entities to aid forensic investigation

Figure 7 shows fluctuations of temporal inflow and outflow of behavioural classification and risk assessment. It monitors the record indices and injects structural and temporal dependencies into the ESWS-Att-GNN model. Determines documentation defects and clusters of entities to be deanonymized.

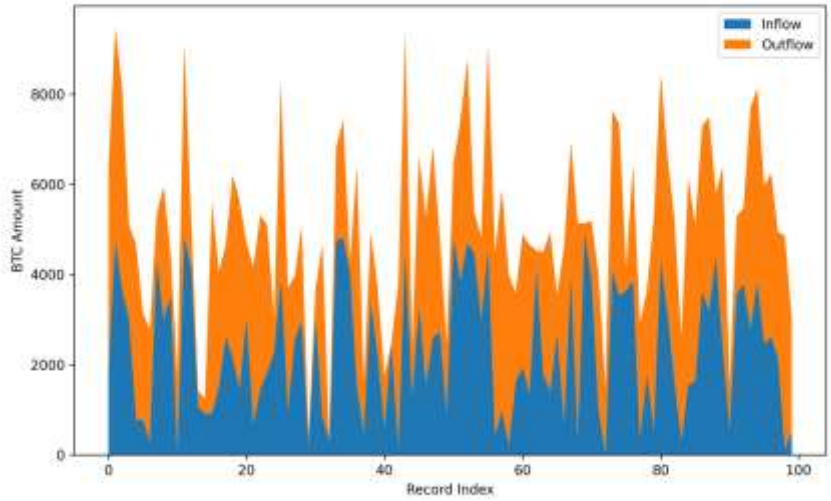

Figure 7: The graphical representation of the flow of transaction of temporal inflow and outflow volumes which is used in the classification of behavior and detection of anomalies used in forensics

5.2 Class-wise Entity Recognition Performance

In order, check the discrimination and performance based of dissimilar behavioral patterns, checking of class-wise performance of each type of entity of Bitcoin, Table 3.

Table 3: Class-wise Precision, Recall, F1 Score Analysis of Bitcoin Entity prediction

Entity Type (Label)	Precision	Recall	F1 Score
Exchange (0)	0.972	0.969	0.970
Mining Pool (1)	0.967	0.962	0.964
Payment Service (2)	0.958	0.952	0.955
Wallet Provider (3)	0.953	0.948	0.950
Mixer / Tumbler (4)	0.944	0.938	0.941
Ransomware (5)	0.941	0.934	0.937
Darknet Marketplace (6)	0.939	0.932	0.935
Scam / Fraud (7)	0.948	0.942	0.945
Gambling (8)	0.950	0.945	0.947
Individual User (9)	0.969	0.964	0.966

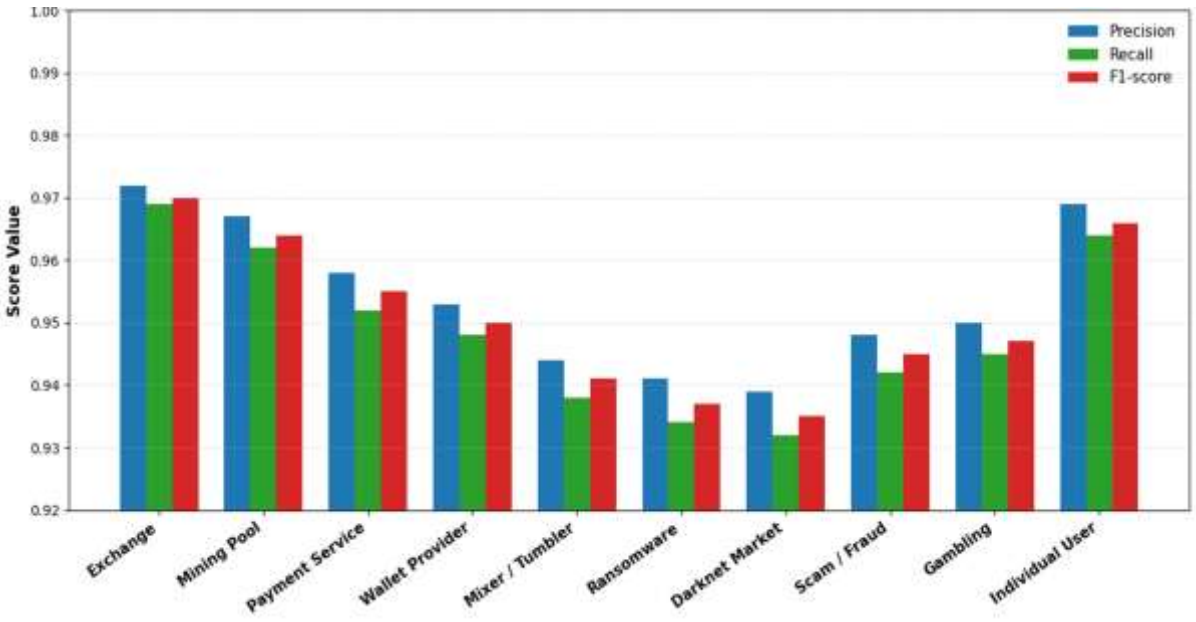

Figure 8: Bitcoin Entity Classification Using ESWS-Att-GNN Model

The ten results of the class-wise classification of the proposed ESWS-Att-GNN model on ten Bitcoin entities categories are summarized in Figure 8. The F1-scores of exchanges and individual user classes are maximum (0.970 and 0.966), which proves the consistency of the transactional behavior. The fact that the scores of illicit entities are slightly lower means that there is more behavior overlap and complexity without compromising on the overall precision and recall.

5.3 Feature Contribution and Behavioral Sensitivity Analysis

The attention-based importance scores portray solely input behavioral attributes that help in entity classification through Table 4. As the targeted variable is entity_label, which is a supervised target variable, it is not included in the feature importance analysis.

Table 4: Attention-Based Feature Importance Analysis for Bitcoin Entity Transaction Attributes

Feature Name	Importance Score
total_inflow_btc	0.186
total_outflow_btc	0.173
tx_count_out	0.142
tx_count_in	0.138
in_out_ratio	0.118
active_duration_days	0.097
temporal_entropy	0.082
avg_tx_value	0.036
address_count	0.028

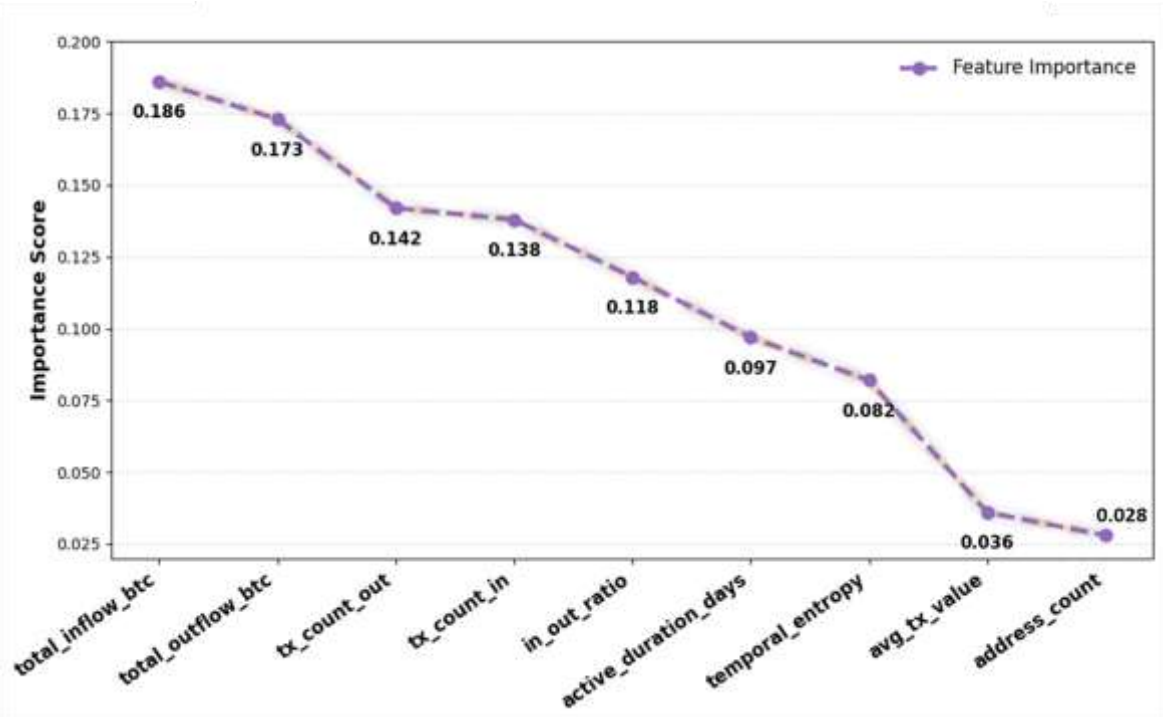

Figure 9: Importance Scores of Bitcoin Transaction Attributes Derived as a result of ESWS-Att-GNN Model

Figure 9 shows attention based feature importance scores as a result of ESWS-Att-GNN model. Inflow (0.186) and outflow (0.173) impact the most, and it means that the pattern of fund movements is dominant. The counts of transactions and flow balance give moderate discrimination, whereas the temporal behavior, average value and address usage give comparatively low though significant classification support.

5.4 Comparative analysis

The results of the analysis of the proposed ESWS-Att-GNN with the current models were compared so as to bring out the entity classification and forensic transaction analysis. The suggested study is compared to

various already known models, which are called the GAN classifier1 [16]. Table 5 is used to compare performance evaluation through standard measures like score, precision, recall, F1 score and MCC.

Accuracy: To assess level in classification, which is the measure of success and accuracy of Bitcoin entity detection models. Percentage scores that specify the model performance in the accuracy, precision, recall, as well as F1-score per individual entity class in Equation 9.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (9)$$

Precision: To estimate the rate of correctly recognized Bitcoin entities in the set of all predicted examples to guarantee an accuracy of classification. In equation (10) Precision improved using GAN-based resampling showing the existence of more accurate identification of minority Bitcoin entity classes.

$$precision = \frac{TP}{TP+FP} \quad (10)$$

The TP stands for True positive, TN stands for True Negative, FP stands for False Positive, and FN stands for False Negative.

Recall: To evaluate capability of the model to identify the presence of Bitcoin entities engaging in illegal activities or those falling in the minorities category. In Equation (11), Recall is measured as the fraction of actual positive entities of Bitcoin, which are correctly classified by the classifier in experiments.

$$Recall = \frac{TP}{TP+FN} \quad (11)$$

F1 Score: To determine the trade-off between precision and recall, determining the effectiveness of the classifier with respect to entity detection of Bitcoin. In Equation (12), minority classes trained with GAN-based resampling had seen an improvement in the F1 Score, which boosted overall entity classification performance.

$$F1 - Score = 2 * \frac{precision*recall}{precision+ recall} \quad (12)$$

MCC: To assess the overall quality of Bitcoin classification of entities taking into consideration all the real and false prediction. Gives one score on correlation to measure model performance, which is a compromise between the performance on majority and minority classes.

Table 5: Comparison of the performance with various metrics of Bitcoin entity classification

Method	Accuracy %	Precision %	Recall %	F1 Score %	MCC %
GAN classifier$_1$[16]	96.64	94.0	90.0	92.0	94.0
ESWS-Att-GNN [Proposed]	98.45	96.0	92.0	95.0	97.0

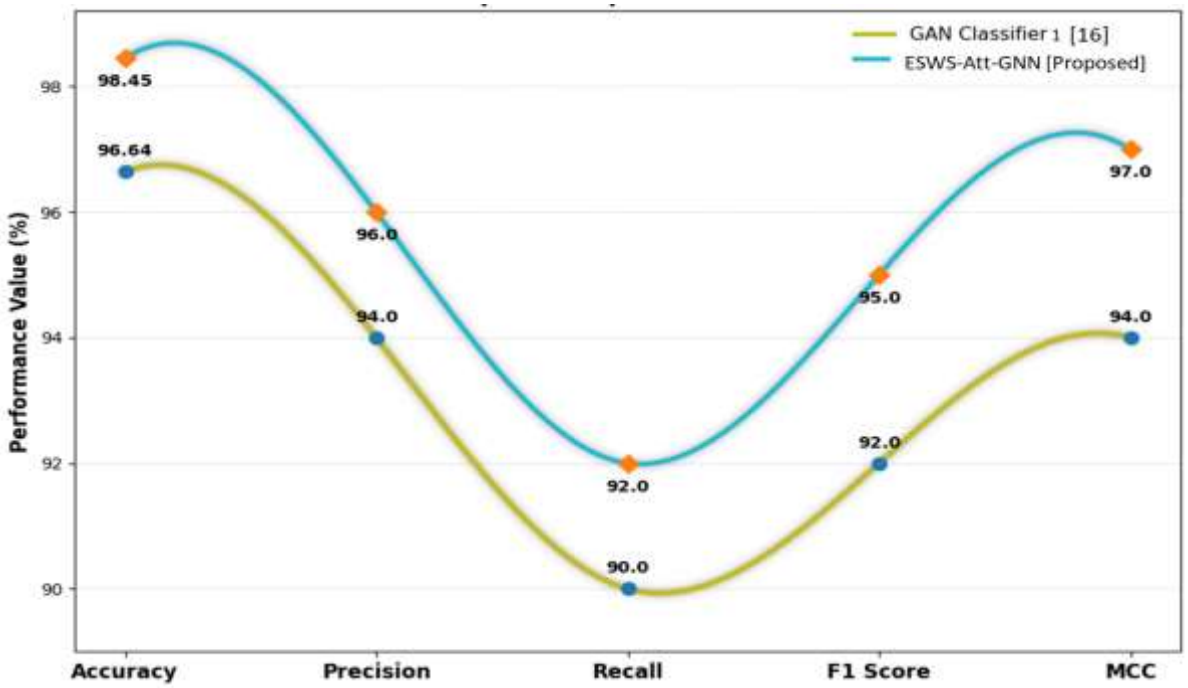

Figure 10: Comparative Evaluation of ESWS-Att-GNN and GAN Classifier Performance Based on Metrics

Table 5 and Figure 10 compare GAN Classifier1 [16] and the proposed ESWS-Att-GNN, which indicate that the latter has a better performance on all metrics, with an accuracy of 98.45%, a precision of 96.0%, a recall of 92.0%, an F1-score of 95.0%, and an MCC of 97.0%, which proves an improved performance of Bitcoin entity classification.

6. Discussion

Researched an automatic deanonymization entity and forensic transaction analysis DL-based blockchain framework of Bitcoin. The current procedures include the GAN classifier1 [16], which tend to have unstable training and cannot form complex graph-based relationships in blockchain transaction networks, which restricts their usefulness in the deanonymization of Bitcoin entities with accuracy. The current study avoids this weakness by incorporating ESWS-Att-GNN, training node embeddings effectively, hyperparameter optimization, and proper classification without depending on artificial GAN-generated images only.

• **Practical implications**: The framework has practical implications in that it facilitates law enforcement, regulators, and exchanges through risk assessment automated, forensic tracing, compliance auditing, and transparent decision accountability across the cryptocurrency ecosystems.

7. Conclusion

This study successfully constructed a coherent DL and blockchain system of entity deanonymization and forensic transaction analysis. It has used the Bitcoin Entity Transaction Dataset and has suggested ESWS-Att-GNN to enhance transparency, security, and regulatory compliance to Bitcoin transaction analysis. The proposed model ESWS-Att-GNN is contrasted with the current model to note the performance and it has achieved the accuracy of 98.45, precision of 96.0, recall of 92.0, F1-score of 95.0 and MCC of 97.0. ESWS-Att-GNN framework is an entity deanonymization and classification framework that enables better forensic analysis and auditability.

Limitations and Future Scope

- **Limitations:** Limitations Reliance on labelled datasets, possible bias in ground truth, scalability limitations on huge graphs and ethical issues (possible privacy, surveillance, and misuse).
- **Future Scope:** Future work will expand the model to multi-chain ecosystems, real-time streaming analytics, adversarial robustness, explainable AI integration and privacy-preserving learning under changing regulatory needs internationally.

Appendix Table

Abbreviation	Description
AML	Anti-Money Laundering
AM	Attention Mechanism
Att-GNN	Attention-based Graph Neural Network
CHetG	Contrastive Heterogeneous Graph-based model
DL	Deep Learning
ESWS	Elephant Swarm Water Search
GPU	Graphics Processing Unit
IP	Internet Protocol
I2P	Invisible Internet Project
MCC	Matthews Correlation Coefficient
ML	Machine Learning
PCP	Parallel Coordinate Plot
RF	Random Forest
XGBoost	Extreme Gradient Boosting
LR	Logistic regression
DT	Decision Trees
RF	Random Forests
GAN	Generative Adversarial Networks

References

1. Zhuk, A., 2024. Crypto-anarchy: a paradigm shift for society and the legal system. Journal of Computer Virology and Hacking Techniques, 20(4), pp.697-723. https://doi.org/10.1007/s11416-024-00525-1
2. Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M.Z., and Ferretti, S., 2023. Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. Electronic Markets, 33(1), p.37. https://doi.org/10.1007/s12525-023-00654-3
3. Thomas, T., Edwards, T. and Baggili, I., 2022. BlockQuery: Toward forensically sound cryptocurrency investigation. Forensic Science International: Digital Investigation, 40, p.301340. https://doi.org/10.1016/j.fsidi.2022.301340
4. Kumar, G., Saha, R., Conti, M. and Kim, T.H., 2025. ZAKON: A decentralized framework for digital forensic admissibility and justification. Information Processing & Management, 62(6), p.104226. https://doi.org/10.1016/j.ipm.2025.104226
5. Tironsakkul, T., Maarek, M., Eross, A. and Just, M., 2022. Context matters: Methods for Bitcoin tracking. Forensic Science International: Digital Investigation, 42, p.301475. https://doi.org/10.1016/j.fsidi.2022.301475
6. Dudani, S., Baggili, I., Raymond, D., and Marchany, R., 2023. The current state of cryptocurrency forensics. Forensic Science International: Digital Investigation, 46, p.301576. https://doi.org/10.1016/j.fsidi.2023.301576
7. Gong, Y., Chow, K.P. and Yiu, S.M., 2025. Improved the Bitcoin simulation model and address heuristic method. Forensic Science International: Digital Investigation, 53, p.301935. https://doi.org/10.1016/j.fsidi.2025.301935
8. Saxena, R., Arora, D., Nagar, V., and Chaurasia, B.K., 2024. Blockchain transaction deanonymization using ensemble learning. Multimedia Tools and Applications, 83(37), pp.84589-84618. https://doi.org/10.1007/s11042-024-19233-5
9. Ouyang, S., Bai, Q., Feng, H. and Hu, B., 2024. Bitcoin money laundering detection via subgraph contrastive learning. Entropy, 26(3), p.211. https://doi.org/10.3390/e26030211
10. Islam, A., Sakib, N., Zhang, K., Wuthier, S. and Chang, S.Y., 2025. Anonymous Networking Detection in Cryptocurrency Using Network Fingerprinting and Machine Learning. Electronics, 14(11), p.2101. https://doi.org/10.3390/electronics14112101
11. Garin, L. and Gisin, V., 2023. Machine learning in classifying bitcoin addresses. The Journal of Finance and Data Science, 9, p.100109. https://doi.org/10.1016/j.jfds.2023.100109
12. Zhao, K., Dong, G. and Bian, D., 2023. Detection of illegal transactions of cryptocurrency based on mutual information. Electronics, 12(7), p.1542. https://doi.org/10.3390/electronics12071542
13. Deuber, D., Gruber, J., Humml, M., Ronge, V. and Scheler, N., 2024. Argumentation Schemes for Blockchain Deanonymisation. FinTech, 3(2), pp.236-248. https://doi.org/10.3390/fintech3020014
14. Lu, G., Li, K., Wang, X., Liu, Z., Cai, Z. and Li, W., 2024. Neural-based inexact graph de-anonymization. High-Confidence Computing, 4(1), p.100186. https://doi.org/10.1016/j.hcc.2023.100186
15. Pérez-Cano, V. and Jurado, F., 2025. Fraud detection in cryptocurrency networks—An exploration using anomaly detection and heterogeneous graph transformers. Future Internet, 17(1), p.44. https://doi.org/10.3390/fi17010044
16. Zola, F., Segurola-Gil, L., Bruse, J.L., Galar, M. and Orduna-Urrutia, R., 2022. Attacking Bitcoin anonymity: generative adversarial networks for improving Bitcoin entity classification. Applied Intelligence, 52(15), pp.17289-17314. https://doi.org/10.1007/s10489-022-03378-7