Sigma Journal of Engineering and Natural Sciences
Web page info: https://sigma.yildiz.edu.tr
DOI: 10.14744/sigma.2026.2019

Research Article

A hybrid deep learning framework with attention mechanism for anti money laundering in cryptocurrency transactions

Emine CENGİZ[1,*], Murat GÖK[1]

[1]*Department of Computer Engineering, Yalova University, Yalova, 77200, Türkiye*

ARTICLE INFO

Article history
Received: 04 October 2024
Revised: 12 November 2024
Accepted 28 January 2025

Keywords:
Anti Money Laundering, Attention Mechanism; Bidirectional Long Short Term Memory; Convolution Neural Network; Deep Learning

ABSTRACT

Bitcoin and other cryptocurrencies are technological innovations that have transformed the world of finance. However, these developments introduce new risks. Because of the relative anonymity these systems offer, money laundering is one of the most significant risks connected to cryptocurrencies. This anonymity makes it more difficult to identify money obtained through illegal means, which in turn makes it possible for criminal operations to continue and grow. As a result, creating efficient techniques to identify and stop money laundering in cryptocurrency transactions has grown in importance as a research challenge. In this study, we suggest a hybrid model based on deep learning to detect illicit money transfers in cryptocurrency transactions. Convolutional Neural Networks (CNN), Bidirectional Long Short-Term Memory Networks (BiLSTM), and an Attention Mechanism are all integrated in the suggested method. CNNs are used in the model's initial stage to extract significant features from the unprocessed data. The BiLSTM layer then received these features in order to identify the dependencies in the sequential data structures. The Attention Mechanism enhances the overall classification performance in the last step by giving the BiLSTM outputs importance weights. The Elliptic dataset was used to assess the suggested model's performance. The experimental results indicate that the model achieves superior performance compared to existing methods, with an accuracy of 97.9%, precision of 99.0%, recall of 98.0%, and F1-score of 98.0%. The findings of this study highlight the effectiveness of deep learning models enriched with Attention Mechanism for detecting illicit activities in cryptocurrency transactions. Beyond presenting a high performing model, its contribution to the literature lies in offering an novel approach to prevent crimes associated with the growing use of cryptocurrencies.

Cite this article as: Cengiz E, Gök M. A hybrid deep learning framework with attention mechanism for anti money laundering in cryptocurrency transactions. Sigma J Eng Nat Sci 2026;44(2):970–982.

***Corresponding author.**
*E-mail address: emine.cengiz@yalova.edu.tr

This paper was recommended for publication in revised form by Editor-in-Chief Ahmet Selim Dalkilic

INTRODUCTION

Black money is defined as earnings obtained through illegal means. Money laundering represents the income obtained as a result of crimes such as drug trafficking, arm smuggling, and human trafficking, as if obtained from legal sources [1, 2]. Money laundering is the root cause of many crimes that use illicit money. It is difficult to estimate the total amount of money laundered each year because of the illegal nature of the transactions. However, [3] states that the revenue obtained through money laundering is between 800 billion and 2 trillion dollars worldwide. Money laundering poses a significant threat to global financial system [4]. Anti Money Laundering (AML) guidelines have been established to prevent harm caused by this activity. To combat money laundering, the European Union adopted the "Fifth Money Laundering Directive (5AMLD)." This law obliges maintaining customer history, monitoring transactions, and reporting any suspicious transactions to money laundering [5].

With the emergence of cryptocurrencies, money laundering evolved technologically. Cryptocurrency is a digital payment system designed in a virtual environment (without a bank) to verify and secure monetary transactions using cryptographic methods. Unlike paper money and financial systems, cryptocurrencies have a decentralized structure. The decentralization of each cryptocurrency originates from the blockchain structure, which acts as a database. It has been reported that money laundering, a criminal crime, is carried out through the blockchain [6, 7].

A rule based system is a basic method employed for detecting money laundering. It consists of a series of conditions that analyze whether specific events have occurred or if certain thresholds have been surpassed, indicating a suspicious state. However, this technique also has several disadvantages. One of its major disadvantages is that it leads to a high false positive rate and requires experts to create rules [8]. Machine learning (ML) methods, on the other hand, overcome the challenge of rule based systems by extracting complex models from historical data and can reduce high false positive and false negative rates [9]. With the emergence of big data, deep learning techniques can be considered as a solution to prevent money laundering [10].

Whereas feature extraction is performed manually in ML methods, the features of the input data are learned automatically in Convolutional Neural Networks (CNN) and Long Short Term Memory (LSTM) [11]. Feature extraction plays a critical role in enhancing the performance of the proposed model and effectively analyzing the dynamic and complex nature of cryptocurrency transactions. Specifically, cryptocurrency transactions are often irregular, high dimensional, and contain time series data. When analyzed directly, such data can negatively impact both the learning process and the classification performance. Feature extraction allows the model to extract meaningful and summarized information from such complex, high dimensional data. The CNN model was applied to f synthetic financial transaction data by Kute et al. [12]. In terms of accuracy and false negative rates, the proposed approach performed better than other machine learning techniques like Random Forest (RF), Support Vector Machine (SVM), and XGBoost. The Shapley Additive exPlanations (SHAP) method was used to make the model outputs easier to understand. The visual analysis of each feature's contribution to the classification process was evaluated by anti-money laundering (AML) specialists. Rani et al. [13] suggested an LSTM-based model to detect and prevent money laundering. This model is designed to support the reporting of suspicious activity and the construction of client risk profiles. By modeling financial data as time series, it becomes possible to detect transaction patterns associated with money laundering. Bidirectional Long Short-Term Memory (BiLSTM) is a deep learning architecture that allows temporal dependencies to be learned from both forward and backward directions. The Attention Mechanism (AM) operates by modulating the contribution of hidden states within sequential representations, assigning greater emphasis to those deemed more informative [14]. In doing so, it reduces the impact of less relevant signals and directs the model's focus toward features that carry stronger discriminative value. Consequently, the learning process becomes more efficient and the overall classification performance improves. Tang et al. [15] proposed the BiLSTM4DPS model to detect phishing scam accounts on the Ethereum network. This model is based on a BiLSTM architecture enhanced with an Attention Mechanism. In their study, features such as transaction amounts and transaction counts were used to analyze the account behavior. This model converts account transaction records into sequences to extract the temporal and latent patterns of transactions. By integrating AM with masking techniques, a classification model is constructed to identify fraudulent accounts. Jainish and Alwin [16] proposed a deep learning based approach for financial fraud detection. The accuracy of fraud detection is improved by using Fisher score based feature selection and BiLSTM with AM. The model processes the data in matrix form to learn temporal dependencies and then focuses on important data through AM. A model for identifying unusual patterns in blockchain transactions was proposed by Wang et al. [17]. In this model, an inception structure was added to the CNN architecture to facilitate the learning of various patterns. To better account for the interactions among learned representations, a self-attention component was incorporated into the architecture, with the aim of refining overall model performance.

Although deep learning approaches have shown promise in the detection of money laundering, many existing implementations remain limited in their ability to represent the structural complexity and evolving dynamics of cryptocurrency transactions. Addressing this gap, the present work develops a hybrid CNN–BiLSTM–AM architecture that integrates convolutional feature extraction,

bidirectional sequence modeling, and an attention mechanism within a unified framework.

In this model, the extraction of local features using CNN and the extraction of sequence features using BiLSTM were combined. AM is then used to dynamically evaluate the importance of each feature in the sample input. The novelty of this study lies in the combination of deep learning techniques and AM to improve the detection of illegal cryptocurrency transactions. Graph based algorithms for AML detection were typically employed in earlier research. This study fills this gap in the literature by showing how deep learning can be effectively used in challenging areas, such as the detection of illegal activities.

The main contributions of this study are summarized as follows:

- In this study, after testing various models, including CNN, LSTM, BiLSTM, and their combinations, the CNN-BiLSTM-AM hybrid model is proposed. This model is designed to detect illegal money transfers and is enhanced by the AM.
- The hybrid model was tested on the Elliptic dataset and achieved superior results compared to existing methods in the literature.
- ·This study indicates that incorporating AM can meaningfully support AML efforts. These results offer insightful direction for further studies meant to reduce the dangers connected to the increasing use of cryptocurrencies.

The structure of this paper is as follows. Section 2 reviews previous studies and methods using an Elliptic dataset. Section 3 discusses the dataset, working principles, and the architecture of the proposed model. The functionality and interactions of each component of the model are described. Section 4 explains the model setup designed in this study and provides the experimental results and performance metrics. A comparison was conducted between the proposed model and alternative methods using an Elliptic dataset. Section 5 provides a discussion of the findings, implications, and limitations of this study. Finally, Section 6 summarizes the key findings of this study.

LITERATURE REVIEW

Recently, research in the field of AML has incorporated graph based algorithms and ML. In this section, a summary of the work conducted for AML using an Elliptic dataset is provided.

One kind of neural network intended for handling and evaluating graph-structured data is the Graph Neural Network (GNN). GNN are capable of handling dynamic structures made up of nodes and edges, whereas traditional neural networks usually work with fixed and regular data structures. GNN are able to model the structural relationships and connectivity patterns of a graph by learning the features of its nodes and edges through the use of neighborhood information. A vast variety of models based on different learning strategies are included in GNN architectures. These consist of the Graph Isomorphism Network (GIN), Graph Attention Network (GAT), Graph Convolutional Network (GCN), and GraphSAGE. GCN is a deep learning model used to recognize and predict patterns on graph based data structures. GCN is a structure adapted to graph data structures based on a CNN. First, Weber et al. [18] proposed an Elliptic dataset in their study and divided the dataset into 70% training and 30% test sets to detect illegal Bitcoin transactions. They used a GCN, Logistic Regression (LR), RF, and Multilayer Perceptron (MLP) to evaluate the dataset and perform binary classification. The results were compared for precision, sensitivity, and F1 score. The RF technique achieved precision, sensitivity, and F1 score of 0.95, 0.67, and 0.78, respectively. Alarab et al. [19] presented a new approach based on MLP and GCN to predict illegal transactions on the Elliptic dataset. In the proposed method, they obtained the result that the hidden representation of GCN derived features and a linear layer increased the performance of the model according to the study [18]. GAT is a deep learning model used to model the relationships between nodes in graph structured data. Pocher et al. [20] used the GCN and GAT methods. This is the first time that GAT has been applied to detect anomalies in Bitcoin. Their results showed that the GCN yielded better results than the GAT. GraphSAGE is a method used for node embedding learning in large scale graphs. Chen et al. [21] proposed a GraphSAGE model that can detect target node features from neighboring features and their time series features. They aimed to detect whether the target node was anomalous to its neighboring nodes. For this purpose, they computed the similarities between the features of neighboring nodes. They also used GraphSAGE to combine the features of neighboring nodes. Deep Graph Infomax (DGI) and GIN are two different GNN methods used for modeling graph data. Lo et al. [22] proposed Inspection-L, a self supervised GNN framework based on DGI and GIN. DGI is a general unsupervised learning approach for acquiring node representations in data with graph structure. The proposed Inspection-L method is based on the combined use of RF and DGI to detect illegal transactions. Additionally, the proposed model allows each node to access all graph structural models by capturing neighborhood information. They used the DGI along with the recommended GIN to learn node placements. Node placements were then evaluated using the RF algorithm for the training and test sets.

Deep learning is an effective tool for solving complex and multidimensional problems such as detecting and preventing money laundering. To address the spatiotemporal complexity of money laundering transactions, Wan and Li [23] proposed a deep learning based prediction model called MDGC-LSTM. The model aims to capture multilayer relationships within transaction data by combining a Dynamic Graph Convolutional Network and LSTM network. It achieved a 25% higher Macro-F1 score compared to the best existing models on the Elliptic dataset. Yang et

al. [24] proposed two methods to solve AML problems. The first method combines the LSTM-GCN algorithms, and the second method uses ensemble learning. A multi-label classification model is trained using the LSTM-GCN algorithm, which improves the detection accuracy of illegal transactions. In the second method, multiple models are trained to identify and separate the illegal transaction data. Xia et al. [25] proposed a hybrid spatiotemporal prediction model based on GCN and LSTM, called MGC-LSTM. Elliptic dataset is a structure consisting of 49 different time steps. The 49 time steps were learned independently and the output of the previous step served as the input for the next step. LSTM was used to obtain the temporal dependence of the dataset, and GCN was used to learn the spatial dependence of its processes. The results trained by the LSTM were provided as inputs to the GCN. Xiao et al. [26] presented a novel method for tuning GCN network parameters, called CTDM, which integrates EvolveGCN with Minimal Gated Unit (MGU). MGU was developed as an alternative to LSTM cells. MGU uses fewer input gates than LSTM cells. In addition, MGU offers a simpler structure by directly applying an additional logistic value to the memory cell and the forget gate. CTDM uses the MGU to improve the parameters of the GCN and requires fewer learning parameters through the MGU. Guo et al. [27] proposed LB-GLAT to capture the topological structure and attribute features of money laundering. LB-GLAT was designed to successfully identify the target of blockchain transactions using a transaction graph and an inverse transaction graph. The problem of over smoothing was reduced using a long term layer attention mechanism. They obtained an accuracy of 97.0%, precision of 93.0%, recall of 84.0%, F1-score of 88.87% and AUC performance of 0.98. Wang et al. [28] proposed the RMGANets method to overcome the limitations of GCN. This method is a reinforcement learning based approach that incorporates multi relational attention graph awareness. In their study, they constructed a large multi relational graph that includes transactions, addresses, users, and cash flows as nodes. Reinforcement learning was utilized to complete the missing node information caused by masking operations and to emphasize the differences between the various types of nodes.

Label scarcity refers to the fact that not all or some examples in the training dataset have class labels. Lorenz et al. [9] studied the lack of labels in an Elliptic dataset. In the dataset, 21% of Bitcoin transactions are labeled as legal and 2% as illegal. The remaining transactions do not contain tag data. The number of labels was increased using Active Learning to improve the performance of unsupervised learning. The classification was performed using XGBoost (76%), LR (45%), and RF (83%). Despite employing a distinct approach to address this issue, the authors did not intend to achieve superior outcomes. Monte Carlo dropout (MC-dropout) is a method used in uncertainty estimation for ML and especially deep learning models. This method is related to a technique known as dropout, which is used to organize a network during learning. Alarab et al. [29] and Alarab and Prakoonwit [30] applied the MC-Dropout method in their studies. In [30], an active learning framework for analyzing the Bitcoin dataset was introduced. They used active learning called Monte-Carlo Dropout (MC-Dropout) and Monte-Carlo Based Adversarial Attack (MC-AA) to calculate uncertainties. They later proposed a temporal-GCN by combining LSTM and GCN models. The results showed that they achieved an accuracy of 97.7%. Jatoth et al. [31] analyzed feature selection to improve classification. The purpose of feature selection is to select fewer or more appropriate features in order to obtain a better model. They applied ensemble and classical supervised learning methods to classify the legal and illegal transactions. Consequently, they achieved better results in community learning models.

A review of AML studies highlights the increasing complexity of money laundering methods and the significant challenges posed by the anonymity of virtual currency transactions to existing methods. The lack of labeled data makes this problem worse and restricts the effectiveness of supervised learning-based models [23]. A range of methods such as GCN, LSTM, and various hybrid or graph-based architectures has been examined in prior research. However, these models often have limited scalability, interpretability, and adaptability to the dynamic nature of cryptocurrency transactions.

This study proposes a novel hybrid model that combines CNN, BiLSTM, and an AM in order to get around these limitations. The attention component directs the model toward the most salient features during classification, combining convolutional feature extraction and bidirectional temporal modeling instead of depending on a single modeling paradigm. By effectively learning both temporal dependencies and structural relationships, the proposed model aims to increase the reliability and accuracy of illicit transaction detection. This method shows a strong performance on complex and large datasets by addressing the shortcomings of previous approaches. This study contributes a significant innovation to the AML field by filling critical gaps in the literature.

MATERIAL AND METHODS

In this section, the dataset used in this study is described. An overview of the existing CNN, BiLSTM, and AM approaches utilized to perform the work is then provided. Finally, the proposed method is described.

Dataset

Elliptic dataset used in this study is a Bitcoin graph, where nodes represent transactions and edges represent flows between transactions [18]. This dataset is recognized as one of the most extensively labeled datasets available for cryptocurrencies [32]. It comprises 49 graph structures sampled from the Bitcoin blockchain at various time

intervals. The dataset consists of 203,769 node processes and 234,355 edges. Each transaction is divided into three classes: legal (e.g., wallet providers, exchanges, legitimate services, and miners), illegal (e.g., terrorist organizations, ransomware, and Ponzi schemes), and unknown. Of the total number of transactions, 2% (4,545) were labeled as illegal and 21% (42,019) as legal. The remaining 77% (157,205) as unknown. The dataset comprises 166 features, with the first 94 features relating to transaction specific information, such as input number, output number, transaction fee, and time step. The remaining 72 features relate to the aggregate information about the direct neighbors of the process, providing the correlation coefficient, standard deviation, and maximum and minimum values of each process.

Convolutional Neural Networks

CNN is a widely utilized artificial neural network architecture within the domain of deep learning [33]. It uses special layers such as convolution and pooling to understand the structure and properties of data. CNN is composed of convolution, activation, pooling, and fully connected layers [34]. The convolution layers enable the generation of feature maps by applying sliding filters over the input data [35]. These feature maps represent different attributes of the input data. Activation layers apply a specific activation function to each generated feature map.. This activation function emphasizes or suppresses the significance of certain features in each feature map based on weights. Pooling layers were used to decrease the dimensions of the feature maps [36]. In practice, pooling operations rely on maximum or average sampling strategies to condense the feature maps. This reduction in dimensionality lowers the number of parameters that must be learned, easing computational requirements while also mitigating the tendency toward overfitting. Once the feature representations have been smoothed in this way, they are passed to fully connected layers, where they are processed within a conventional neural network structure for final classification or prediction. These layers ultimately generate the final outputs by leveraging the features learned by the CNN in earlier stages.

Bidirectional Long Short Term Memory

Recurrent Neural Networks (RNN) are deep learning models that operate based on prior knowledge of data [37]. The basic component of RNN is their cell structure. The cells process the inputs and previous outputs while maintaining their internal states. The RNN uses these cells at each time step, and the outputs of these cells are provided as inputs for the next step. Feedback algorithms are another important component of RNN. This algorithm identifies the source of the error and optimizes network parameters. Feedback is important to reduce errors during network training. Another RNN variation is the LSTM network [38]. LSTM uses sequential data as the input and makes predictions by remembering the information held at the previous time steps. Thus, LSTM is highly successful at processing complex sequential data. The LSTM cell consists of a mechanism comprising a forget, input gates, output gates, and cell state. Figure 1 shows the LSTM structure.

Forget gate in a RNN is responsible for determining which information from the previous hidden layer and current input will be retained or forgotten. This is achieved by passing the combined information from the previous hidden layer and current input through a sigmoid function.

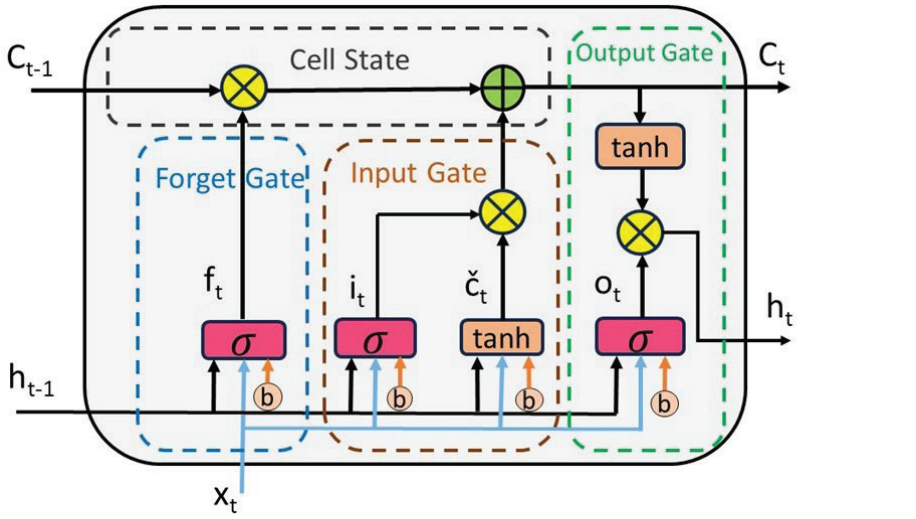

Figure 1. LSTM structure.

Information from the input. X_t and the previous output h_{t-1} are passed through the sigmoid function. The sigmoid function outputs a value between 0 and 1, where a value close to 0 indicates that the information will be largely forgotten and a value close to 1 indicates that the information will be retained. The forget gate [39, 40] f_t is given by Equation 1.

$$f_t = \sigma(W_f . [h_{t-1}, x_t] + b_f) \quad (1)$$

Input gate is used to update the cell state. First, a sigmoid function is applied, and the information that will be retained is determined. The output of the sigmoid function is reduced between -1 and 1 using the tanh function. This process normalizes the output of the cell and helps the network operate more stably. The cell state was updated by multiplying the two values obtained. This new memory was added to the C_{t-1} memory to obtain the C_t. In Equation 2, the sigmoid function, and in Equation 3, the tanh function steps are given.

$$i_t = \sigma(W_i . [h_{t-1}, x_t] + b_i) \quad (2)$$

$$\check{C}_t = tanh\,(W_C . [h_{t-1}, x_t] + b_C \quad (3)$$

The most important task for the Cell State in a cell is to carry information. It receives data that must be passed on to the end of the cell, and then to other cells. First, the Forget Gate output was multiplied by the output of the previous layer. Next, it is added to the value from the input gate. These operations update the state of the cell and allow relevant information to be transmitted to the next cell. The new cell state [39, 40] C_t is given by Equation 4.

$$C_t = f_t * C_{t-1} + i_t * \check{C}_t \quad (4)$$

Output Gate determines the value to be sent to the next layer. This value was used for the prediction. At this stage, the previous output (value) and the current input are fed into a third sigmoid function. The Cell State value passes through the tanh function. The output of the tanh function and the result of the sigmoid function were multiplied. The resulting value goes to the next layer as the "previous value." Equation 5 shows the output cell state o_t and Equation 6 shows the output value h_t [39, 40].

$$o_t = \sigma(W_o[h_{t-1}, x_t] + b_o \quad (5)$$

$$h_t = o_t * tan\,h(C_t) \quad (6)$$

BiLSTM is an improved version of the LSTM algorithm [41]. Although the LSTM architecture is unidirectional, the BiLSTM architecture is bidirectional. BiLSTM consists of two LSTM layers: one processing the input in the forward direction, and the other in the backward direction. LSTM can make predictions using historical data, whereas BiLSTM can make predictions using historical and future data. BiLSTM network structure consists of four layers: Input Layer, Forward Layer, Backward Layer and Output Layer. Figure 2 shows the structure of the BiLSTM.

In BiLSTM, the input data sequence (x_{t-1}, x_t, x_{t+1}) is used as the input for both forward and backward LSTM. At each step t, the forward LSTM hidden state ($\vec{h}_t$) and backward LSTM hidden state ($\overleftarrow{h}_t$) were calculated simultaneously. The output h_t of the BiLSTM is calculated using both $\vec{h}_t$ and $\overleftarrow{h}_t$ information. Equations [7-9] calculate the values of $\vec{h}_t$, $\overleftarrow{h}_t$ and h_t [42].

$$\vec{h}_t = f((w_1 x_t + w_2 \vec{h}_{t-1})) \quad (7)$$

$$\overleftarrow{h}_t = f((w_3 x_t + w_5 \overleftarrow{h}_{t+1})) \quad (8)$$

$$h_t = g((w_4 \vec{h}_t + w_6 \overleftarrow{h}_t)) \quad (9)$$

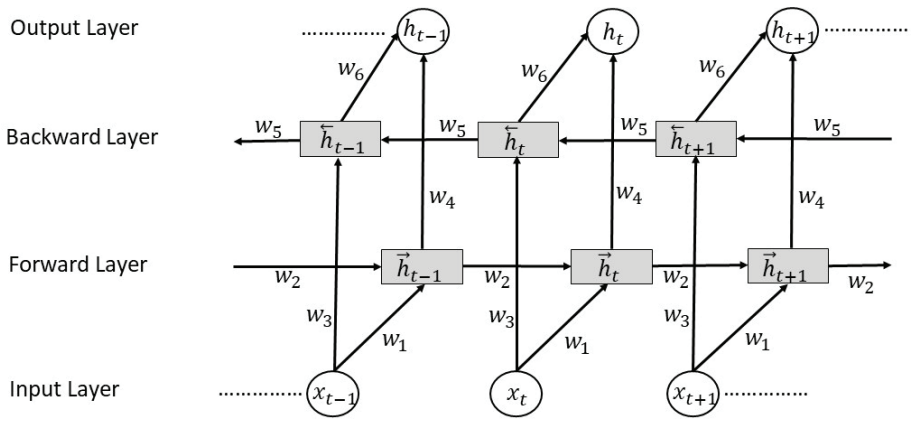

Figure 2. BiLSTM structure.

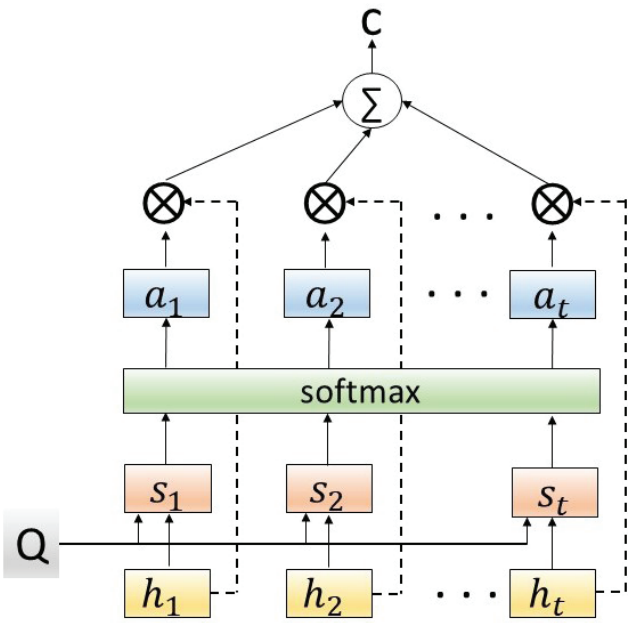

Figure 3. AM structure.

Attention Mechanism

AM refers to a mechanism in deep learning models that allows them to focus on a particular input [43]. This makes the model better able to perform a particular task, and helps it use fewer computational resources. As shown in Figure 3, the AM computational process consists of three stages.

1. Attention score (s_t): The similarity or relationship between input and output features is measured by the attention score. The model uses this score to decide which input features to prioritize. Thus, the attention score emphasizes which input features are more important to the model when generating the output. The attention score [44] is calculated using Equation 10.

$$s_t = tanh\,(W_h h_t + b_h) \tag{10}$$

Where W_h, h_t and b_h are the weight, input vector and deviation of the AM, respectively.

Attention scores determine which input items the model prioritizes, allowing the model to focus on its resources. Inputs associated with lower attention scores are treated as less influential, whereas those with higher scores receive greater emphasis during processing. This enables the model to concentrate on salient information while minimizing the impact of irrelevant, noisy, or redundant inputs.

2. Attention weight (at): Indicates the importance of a particular input item or component, and the attention weight value is calculated using Equation 11 [45].

$$a_t = \text{softmax}\big(s(h_t, Q)\big) = \frac{\exp(s(h_t,Q))}{\sum_t \exp(s(h_t,Q))'} \tag{11}$$

Softmax is commonly used to calculate attention weights. The sum of these weights, which have values ranging from 0 to 1, is 1. This property allows the mechanism to evaluate different input features systematically and assign stronger importance to those most relevant to the decision-making process.

Context vector (c): Context vector enables the model to focus on the input elements that are considered more important. Critical information in the data can be more effectively represented in this way. The context vector is obtained by combining the input elements weighted by their corresponding attention weights [46].

$$c = \sum_t a_t h_t \tag{12}$$

Proposed Model

In this study, the CNN-BiLSTM-AM model is proposed, which combines the features of CNN, BiLSTM, and AM to detect licit and illicit transactions in the Elliptic dataset. The structure of the CNN-BiLSTM-AM model is illustrated in Figure 4. This model consists of the input layer, CNN layer, BiLSTM layer, AM layer and output layer.

In the following, each block of the proposed method is described in detail:

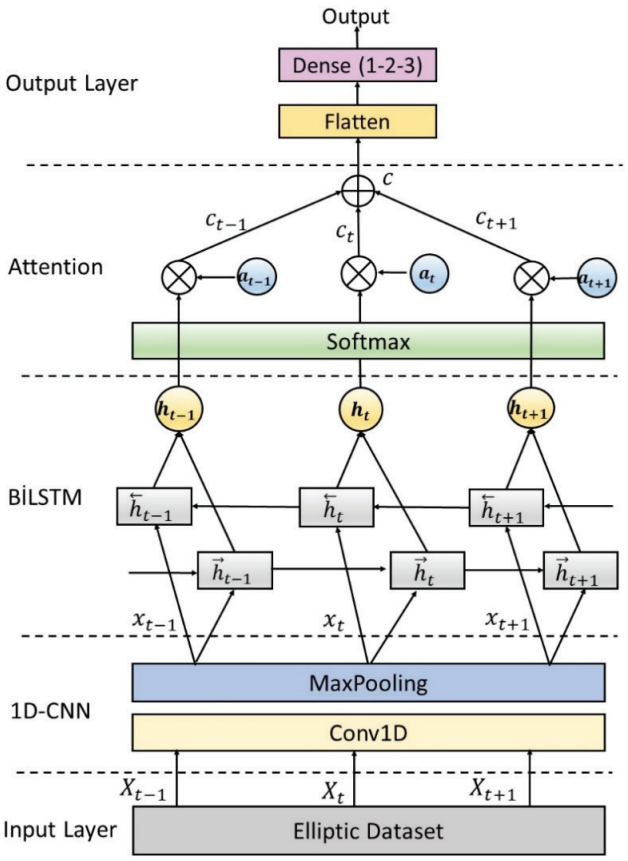

Figure 4. Proposed model.

Input Layer represents the data of cryptocurrency transactions. The data is expressed as time series and is represented as (X_{t-1}, X_t and X_{t+1}) over a specific time period.

CNN is utilized to extract features from the time series data. To extract important features from the input data, sliding filters are applied. The features taken from the CNN layer are further summarized using MaxPooling.

BiLSTM is employed to capture the sequential dependencies in the time series data. The outputs at each time step ($t-1$, $t+1$) are processed based on both past and future information. $\overrightarrow{h}$ and $\overleftarrow{h}_t$ represent the hidden states processed in the forward and backward directions, respectively. The goal of this bidirectional processing is to record the data's context in both directions.

Attention Layer added to the end of the BiLSTM block, this layer assigns different weights to hidden states that contribute differently to the cryptocurrency transactions. This makes it easier to create a high level vector that compiles all pertinent data.

Output Layer flattens the context vectors that the AM produced into a single vector. The final classification is then carried out by one or more fully connected layers using this flattened vector as input.

The parameters of the methods used in the model are provided in Table 1.

Table 1. Parameters of CNN-BiLSTM-AM method

Parameters	Value
Conv1D filters	64
Conv1D kernel size	1
Conv1D activation function	Relu
Conv1D padding	Same
Maxpooling pool_size	2
BiLSTM units	64
BiLSTM activation function	Relu
Attention	-
Dense1 neurons number	64
Dense2 neurons number	32
Dense3 neurons number	1
Training Parameters	**Value**
Optimizer	RMSprop
Epochs	100
Batch_size	64
Loss function	binary-crossentropy

EXPERIMENTAL RESULTS

In this section, the performance results of the CNN-BiLSTM-AM hybrid method applied to the Elliptic datasets used in this study are presented and compared with other studies. The impact of random data splits on performance outcomes was utilized by using the k-fold cross-validation technique. This method involves dividing the dataset into k parts, with each part serving as the test set in a rotation. The remaining data were used to train the model. This process was repeated by creating different combinations of the training and test sets in each cycle. Consequently, the model's performance consistency across various data splits was assessed more reliably. In this study, k is set to 10. The dataset was divided into ten equal parts, and one part was reserved as the test data. The nine parts that remained were trained. The test data was used to assess the models' performance.

Of the total number of transactions, 21% (42,019) are labeled legal, 2% (4,545) are labeled illegal, and the remaining 77% (157,205) are unknown. The dataset's imbalance was addressed using the Synthetic Minority Oversampling Technique (SMOTE) [47]. By reproducing the samples from the minority class, SMOTE balances the dataset. The SMOTE process includes the following steps:

1. A sample belonging to the minority class is selected.
2. A random sample is selected and a vector is created between these two samples.
3. Using this vector to generate new instances, synthetic instances with similarities to the original instance are generated.
4. New synthetic instances are added as part of the original minority class.

SMOTE method was used for k-fold cross validation, where the dataset was balanced at each of the k-folds, and k-fold cross validation was performed on the dataset at each fold separately. This approach ensured that the model at each stage was trained on balanced data. Performance of the hybrid method was then evaluated using accuracy, sensitivity, precision, and F1-score metrics. These values were calculated using Equation 13–16. Performance metrics were obtained from the confusion matrix presented in Table 2.

In the confusion matrix, True Positive (TP) represents an illicit instance accurately identified as illicit. False Positive (FP) refers to a licit instance mistakenly classified as illicit. False Negative (FN) denotes an illicit instance incorrectly identified as licit, while True Negative (TN) represents a licit instance correctly identified as a licit. Accuracy, precision, recall, and F1-score were obtained using the confusion matrix.

Table 2. Confusion matrix

		Predicted Class	
		Positive	**Negative**
Actual Class	**Positive**	**TP**	**FN**
	Negative	**FP**	**TN**

Accuracy: The percentage of correctly classified samples.

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+TN+FN} \quad (13)$$

Precision: The proportion of true positives among the samples predicted as positive. This value measures the success of the correct predictions.

$$\text{Precision} = \frac{TP}{TP+FP} \quad (14)$$

Recall: The metric shows the number of values that need to be estimated as positive and are correctly estimated as positive. If this value is extremely low, illicit transactions cannot be detected effectively.

$$\text{Recall} = \frac{TP}{TP+FN} \quad (15)$$

F1 Score: The harmonic mean of the precision and recall values.

$$F_1 - \text{score} = 2 * \frac{\text{precision} * \text{recall}}{\text{precision} + \text{recall}} \quad (16)$$

Table 3 shows the comparison of the proposed hybrid model with other standalone deep learning methods. CNN is effective in capturing local patterns within the data. BiLSTM is unique in its ability to comprehend relationships that change over time. Together, these two models allow for the simultaneous learning of the temporal dependencies and structural features in the data. By enabling the model to concentrate on the most crucial aspects of the data, the AM further improves the classification accuracy. This feature offers a significant benefit, particularly given the dynamic nature of cryptocurrency transactions. AM enables the model to discard irrelevant data and focus only on meaningful patterns. The proposed model in this study has a structure that enhances the performance of each of the CNN, BiLSTM, and hybrid methods.

The CNN-BiLSTM-AM model delivered the top performance in precision, recall, and F1-score, with values of 99%, 98%, and 98%, respectively, as shown in Table 4 Additionally, an accuracy of 97.9% was obtained, representing the second-highest result in the comparison. Although the Ensemble (Boosting-CFS) method [31] reported the highest overall accuracy, the CNN-BiLSTM-AM model achieved stronger precision, recall, and F1-score values, indicating a more balanced classification of both positive and negative classes.. Although the LB-GLAT method [27] showed 97.76% accuracy, the proposed model exceeded this success with 99.0% accuracy. GCN + MLP [19] and Temporal-GCN [30], which are among the graph based methods, achieved results close to those of the proposed model with 97.4% and 97.7% accuracy values, respectively. While RMGANets [28] has high performance in accuracy 97.96%, the CNN-BiLSTM-AM model still achieves a higher overall balance between all metrics, confirming its better performance in classifying both positive and negative instances. These results demonstrate the superiority of the AM and hybrid architecture of the proposed model for understanding complex data structures. In general, it is observed that the proposed model achieves more effective results than the methods in the literature.

DISCUSSION

In this study, the CNN-BiLSTM-AM hybrid model developed to detect illicit money transfers was tested on the Elliptic dataset. With a precision of 97.62%, the CNN model exhibited a high level of ability to extract features from raw data; however, its recall remained at 91.09%. With a recall of 90.18% and a relatively low precision of 86.49%, the BiLSTM model successfully captured the temporal dependencies in the sequential data.

The CNN-BiLSTM model achieved a high precision of 98.7% by combining the advantages of both methods; however, its recall was only 64.4%. In contrast, the proposed CNN-BiLSTM-AM model, which was improved by incorporating the AM, performed better and more

Tablo 3. Performance comparison of proposed hybrid model and standalone methods

Method	(%) Precision	(%) Recall	(%) F1-score	(%) Accuracy
CNN	97.62	91.09	83.79	96.53
LSTM	65.04	84.75	68.0	91.82
BİLSTM	86.49	90.18	78.10	94.32
CNN+LSTM	73.33	84.78	78.58	95.46
CNN+BİLSTM	98.7	64.40	77.9	96.45
CNN+AM	71.27	82.45	75.87	94.74
BİLSTM+AM	50.78	66.67	56.58	92.43
CNN-BiLSTM-AM	**98.0**	**98.0**	**97.9**	**99.0**

Table 4. The comparison results of CNN+BiLSTM-AM and other methods on elliptic dataset

Reference	Method	(%) Precision	(%) Recall	(%) F1-score	(%) Accuracy
Weber et al. [18]	GCN	81.2	51.2	62.8	
	Skip-GCN	81.2	62.3	70.5	
	EvolveGCN	85.0	62.4	72.0	
Alarab et al. [19]	GCN + MLP	89.9	67.8	77.3	97.4
Pocher et al. [20]	GCN (tx)	90.6	79.0	84.4	-
	GAT (tx)	89.7	60.5	72.3	
Chen et al. [21]	GraphSAGE	61.8	80.2	66.1	91.3
Lo et al. [22]	Inspection-L	97.2	72.1	82.8	-
Yang et al. [24]	LSTM+GCN	85.4	71.2	77.6	-
Xia et al. [25]	MGC-LSTM	96.9	84.4	90.2	
Xiao et al. [26]	CTDM	85.1	87.4	83.5	-
Guo et al. [27]	LB-GLAT	93.17	84.94	88.87	97.76
Wand et al. [28]	RMGANets	96.82	91.32	93.85	**97.96**
Alarab et al. [29]	MC-dropout	-	-	72.9	96.6
Alarab and Prakoonwit [30]	Temporal-GCN	92.7	71.3	80.6	97.7
Jatoth et al. [31]	Ensemble (Boosting-CFS)	98.0	93.0	95.0	**98.0**
	Ensemble (Stacking-CFS)	98.0	92.0	92.0	**98.0**
Proposed Model	**CNN+BiLSTM+AM**	**99.0**	**98.0**	**98.0**	**97.9**

evenly, achieving 97.9% F1-score, 98.0% precision, and 98.0% recall. When considered in relation to earlier studies, these results suggest performance at a state-of-the-art level.

Class imbalance was handled through the application of SMOTE within each fold of the cross-validation process, so that resampling was confined to the training data in every iteration. Embedding this step directly into the validation procedure helped prevent inflated performance estimates and supported a more stable assessment across folds. In this sense, the resulting performance patterns suggest that the model behaves consistently under both conceptual expectations and practical data conditions.

The empirical results show that the CNN–BiLSTM–AM framework maintains stable performance in identifying illicit cryptocurrency transactions, without introducing excessive computational burden. Rather than functioning solely as a high-performing predictive model, the framework also provides insight into how attention mechanisms interact with temporal and structural features in complex classification settings. Future research aimed at better understanding and reducing the risks associated with the growing adoption of cryptocurrencies is anticipated to be guided by this study's findings.

CONCLUSION

Cryptocurrencies represent technological advancements that have significantly altered the financial systems of nations. However, this transformation has also contributed to an increase in illicit activities in the financial domain. In particular, money laundering, terrorist financing, and similar crimes have become more serious threats as cryptocurrencies have been adopted more widely. Consequently, AML in cryptocurrency systems has become a priority issue in the financial sector. In this context, increasing transaction transparency is important. In addition, regulatory policies and compliance mechanisms aimed at strengthening identity verification processes must be developed. Artificial intelligence-based methods are considered effective tools for detecting suspicious transactions and money laundering activities.

This study introduces a method for identifying illegal activities within cryptocurrency transactions. At the same time, the study is intended to offer practical insight into addressing financial crime. The model developed in this study may serve as a reference structure for financial institutions seeking to strengthen their AML strategies. Given its compatibility with blockchain based environments, it also points to possible improvements in transparency and operational security within financial systems. These results are expected to shed light on future research that aims to meet the growing needs of the financial ecosystem and create a safer digital environment from ethical, societal, and economic perspectives.

The findings suggest that the proposed model is not only technically robust but also practically viable for detecting illicit activity. Nevertheless, evaluating its performance across diverse datasets remains important for assessing generalizability, particularly in view of constraints related

to dataset size and structural characteristics. Further investigation is needed to analyze optimization strategies and computational requirements more systematically, particularly in assessing the practicality of real-time deployment.

Against the backdrop of the growing transformation of Bitcoin within the financial ecosystem, this study explores how deep learning techniques can be applied to the detection of illicit activities. The CNN-BiLSTM-AM hybrid model developed in this study offers a novel approach for achieving this goal. As a result of the experiments on the elliptic dataset, it was observed that the model performed better than the other methods in the literature. The results indicate that deep learning techniques can be effective tools in the fight against AML and can make a significant contribution to combating financial crimes. It is also believed that this study will inspire further research and development efforts to understand and address the risks associated with the increasing use of cryptocurrencies.

ACKNOWLEDGEMENTS

This study was supported by Scientific and Technological Research Council of Turkey (TUBITAK, Grant No: 123E312) within the scope of the TUBITAK 1002-A support program.

AUTHORSHIP CONTRIBUTIONS

The authors confirm their contribution to the paper as follows: study conception and design: Cengiz and Gök; data collection: Gök; analysis and interpretation of results: Cengiz and Gök; draft manuscript preparation: Cengiz and Gök. All authors reviewed the results and approved the final version of the manuscript.

DATA AVAILABILITY STATEMENT

The public dataset https://www.kaggle.com/datasets/ellipticco/elliptic-data-set

CONFLICT OF INTEREST

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

ETHICS

There are no ethical issues with the publication of this manuscript.

STATEMENT ON THE USE OF ARTIFICIAL INTELLIGENCE

Artificial intelligence was not used in the preparation of the article.

REFERENCES

[1] Firmansyah W, Atmadja HT. Juridical analysis awareness of profession advocacy to financial transaction reports and analysis centre (PPATK) during prevent and eradicate money laundering crime. J Multidiscip Acad 2021;5:308–314.

[2] Soltani R, Nguyen UT, Yang Y, Faghani M, Yagoub A, An A. A new algorithm for money laundering detection based on structural similarity. In: Proceedings of the 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON); 2016. p. 1–7. [CrossRef]

[3] Bieler SA. Peeking into the house of cards: Money laundering, luxury real estate, and the necessity of data verification for the Corporate Transparency Act's beneficial ownership registry. Fordham J Corp Finan Law 2022;27:193.

[4] Schneider F, Windischbauer U. Money laundering: Some facts. Eur J Law Econ 2008;26:387-404. [CrossRef]

[5] Ahmed AAA. Anti-money laundering recognition through the gradient boosting classifier. Acad Account Financ Stud J 2021;25:1–11.

[6] Bryans D. Bitcoin and money laundering: Mining for an effective solution. Indiana Law J 2014;89:441.

[7] Van Wegberg R, Oerlemans JJ, van Deventer O. Bitcoin money laundering: Mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. J Financ Crime 2018;25:419–435. [CrossRef]

[8] Jullum M, Løland A, Huseby RB, Anonsen G, Lorentzen J. Detecting money laundering transactions with machine learning. J Money Laund Control 2020;23:173–186. [CrossRef]

[9] Lorenz J, Silva MI, Aparício D, Ascensão JT, Bizarro P. Machine learning methods to detect money laundering in the bitcoin blockchain in the presence of label scarcity. In: Proceedings of the 1st ACM International Conference on AI in Finance; 2020. p. 1–8. [CrossRef]

[10] Jensen RIT, Iosifidis A. Qualifying and raising anti-money laundering alarms with deep learning. Expert Syst Appl 2023;214:119037. [CrossRef]

[11] Aggarwal K, Mijwil MM, Al-Mistarehi AH, Alomari S, Gök M, Alaabdin AMZ, et al. Has the future started? The current growth of artificial intelligence, machine learning, and deep learning. Iraqi J Comput Sci Math 2022;3:115–123. [CrossRef]

[12] Kute DV, Pradhan B, Shukla N, Alamri A. Explainable deep learning model for predicting money laundering transactions. Int J Smart Sens Intell Syst 2024;17. [CrossRef]

[13] Rani K, Deepak B, Hemanthh P, Mohanasudhan B, Sathishkumar G. Spatio-temporal network based bank transactional behaviour analysis to detect

suspicious activities. In: Proceedings of the 2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA); 2024. p. 1-6. [CrossRef]

[14] Wang Y, Huang M, Zhu X, Zhao L. Attention-based LSTM for aspect-level sentiment classification. In: Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing; 2016. p. 606–615. [CrossRef]

[15] Tang M, Ye M, Chen W, Zhou D. BiLSTM4DPS: An attention-based BiLSTM approach for detecting phishing scams in ethereum. Expert Syst Appl 2024;256:124941. [CrossRef]

[16] Jainish GR, Alwin Infant P. Attention layer integrated BiLSTM for financial fraud prediction. Multimed Tools Appl 2024;83:80613–80629.

[17] Wang Z, Ni A, Tian Z, Wang Z, Gong Y. Research on blockchain abnormal transaction detection technology combining CNN and transformer structure. Comput Electr Eng 2024;116:109194. [CrossRef]

[18] Weber M, Domeniconi G, Chen J, Weidele DKI, Bellei C, Robinson T, et al. Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics. arXiv [Preprint] 2019:arXiv:1908.02591.

[19] Alarab I, Prakoonwit S, Nacer MI. Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain. In: Proceedings of the 2020 5th International Conference on Machine Learning Technologies; 2020. p. 23-27. [CrossRef]

[20] Pocher N, Zichichi M, Merizzi F, Shafiq MZ, Ferretti S. Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. Electron Mark 2023;33:37. [CrossRef]

[21] Chen C, Li Q, Chen L, Liang Y, Huang H. An improved GraphSAGE to detect power system anomaly based on time-neighbor feature. Energy Rep 2023;9:930–937. [CrossRef]

[22] Lo WW, Kulatilleke GK, Sarhan M, Layeghy S, Portmann M. Inspection-L: Self-supervised GNN node embeddings for money laundering detection in bitcoin. Appl Intell 2023;53:19406–19417. [CrossRef]

[23] Wan F, Li P. A novel money laundering prediction model based on a dynamic graph convolutional neural network and long short-term memory. Symmetry 2024;16:378. [CrossRef]

[24] Yang G, Liu X, Li B. Anti-money laundering supervision by intelligent algorithm. Comput Secur 2023;132:103344. [CrossRef]

[25] Xia P, Ni Z, Xiao H, Zhu X, Peng P. A novel spatiotemporal prediction approach based on graph convolution neural networks and long short-term memory for money laundering fraud. Arab J Sci Eng 2021;47:1921–1937. [CrossRef]

[26] Xiao L, Han D, Li D, Liang W, Yang C, Li KC, et al. CTDM: Cryptocurrency abnormal transaction detection method with spatio-temporal and global representation. Soft Comput 2023;27:11647–11660. [CrossRef]

[27] Guo C, Zhang S, Zhang P, Alkubati M, Song J. LB-GLAT: Long-term bi-graph layer attention convolutional network for anti-money laundering in transactional blockchain. Mathematics 2023;11:3927. [CrossRef]

[28] Wang Q, Tsai WT, Du B. RMGANets: Reinforcement learning-enhanced multi-relational attention graph-aware network for anti-money laundering detection. Complex Intell Syst 2025;11:5. [CrossRef]

[29] Alarab I, Prakoonwit S, Nacer MI. Illustrative discussion of mc-dropout in general dataset: Uncertainty estimation in bitcoin. Neural Process Lett 2021;53:1001–1011. [CrossRef]

[30] Alarab I, Prakoonwit S. Graph-based LSTM for anti-money laundering: Experimenting temporal graph convolutional network with bitcoin data. Neural Process Lett 2023;55:689–707. [CrossRef]

[31] Jatoth C, Jain R, Fiore U, Chatharasupalli S. Improved classification of blockchain transactions using feature engineering and ensemble learning. Future Internet 2021;14:16. [CrossRef]

[32] Alarab I, Prakoonwit S, Nacer MI. Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain. In: Proceedings of the 2020 5th International Conference on Machine Learning Technologies; 2020. p. 23–27. [CrossRef]

[33] Mijwil MM, Aggarwal K, Doshi R, Hiran KK, Gök M. The distinction between R-CNN and Fast R-CNN in image analysis: A performance comparison. Asian J Appl Sci 2022;10. [CrossRef]

[34] Baysal K, Taskin D. Blocking harmful images with a deep learning based next generation firewall. Sigma J Eng Nat Sci 2024;42:1133–1147. [CrossRef]

[35] Cengiz E, Yaylak F, Gülbandılar E. Investigation of polyps in endoscopy images by using deep learning algorithm. Eskisehir Osmangazi Univ J Eng Archit 2022;30:441–453. [CrossRef]

[36] Cihan M, Uzbaş B, Ceylan M. Fusion and CNN based classification of liver focal lesions using magnetic resonance imaging phases. Sigma J Eng Nat Sci 2023;41:119–129. [CrossRef]

[37] Pascanu R, Gulcehre C, Cho K, Bengio Y. How to construct deep recurrent neural networks. arXiv [Preprint] 2013:arXiv:1312.6026.

[38] Sherstinsky A. Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network. Physica D 2020;404:132306. [CrossRef]

[39] Chen L, Zhang W, Ye H. Accurate workload prediction for edge data centers: Savitzky-Golay filter, CNN and BiLSTM with attention mechanism. Appl Intell 2022;52:13027–13042. [CrossRef]

[40] Chen Y, Fang R, Liang T, Sha Z, Li S, Yi Y, et al. Stock price forecast based on CNN-BiLSTM-ECA model. Sci Program 2021;2021:2446543. [CrossRef]

[41] Schuster M. Acoustic model building based on non-uniform segments and bidirectional recurrent neural networks. In: Proceedings of the 1997 IEEE International Conference on Acoustics, Speech, and Signal Processing; 1997. p. 3249–3252. [CrossRef]

[42] Ren F, Jiang Z, Wang X, Liu J. A DGA domain names detection modeling method based on integrating an attention mechanism and deep neural network. Cybersecurity 2020;3:4. [CrossRef]

[43] Niu Z, Zhong G, Yu H. A review on the attention mechanism of deep learning. Neurocomputing 2021;452:48–62. [CrossRef]

[44] Kavianpour P, Kavianpour M, Jahani E, Ramezani A. A CNN-BiLSTM model with attention mechanism for earthquake prediction. J Supercomput 2023;79:19194–19226. [CrossRef]

[45] Li R, Ye X, Yang F, Du KL. ConvLSTM-Att: An attention-based composite deep neural network for tool wear prediction. Machines 2023;11(2):297. [CrossRef]

[46] Tian Y, Wen J, Yang Y, Shi Y, Zeng J. State-of-health prediction of lithium-ion batteries based on CNN-BiLSTM-AM. Batteries 2022;8:155. [CrossRef]

[47] Gökçen T, Odabaş A. Cryptocurrency price prediction using GPR and SMOTE. Sigma J Eng Nat Sci 2024;42:1448–1458. [CrossRef]