The Parallel GRU-LSTM Neural Networks for Accurate Detection of Fraudulent Bitcoin Transactions

Fazell Nasiri
Computer Science department
Rouzbahan Institute of Higher Education,Sari, Mazandaran
Sara Farzai
Computer Science department
Rouzbahan Institute of Higher Education,Sari, Mazandaran Email@daneshpajoohan.ac.ir

Abstract

The Financial fraud continues to rise alarmingly, even as technological advancements strive to address it. This paradoxical trend stems primarily from inadequate coordination among organizations and privacy concerns, which impede access to reliable and comprehensive transaction data. To tackle this challenge, this study introduces an innovative blockchain-based framework designed to detect fraud effectively by leveraging cutting-edge technologies. The proposed system integrates deep learning and machine learning techniques into a cohesive model, enabling robust analysis of transactional data. By constructing a detailed graph representation of sequential transactions on the Bitcoin blockchain, the model identifies patterns, extracts meaningful features, and classifies them to detect suspicious or fraudulent activities. Central to this approach is the Parallel Model, which combines two advanced sequential architectures, namely the Gated Recurrent Unit (GRU) and Long Short-Term Memory (LSTM). These architectures work collaboratively to capture complementary features from time-series input data, ensuring a comprehensive understanding of the temporal and sequential patterns inherent in blockchain transactions. Additionally, the system incorporates the XGBoost algorithm, a powerful feature selection technique, to enhance classification performance. This integrated approach optimizes the model's accuracy in identifying fraudulent transactions, offering a scalable and reliable solution to combat financial fraud in blockchain ecosystems..

Keywords: Bitcoin, Blockchain, Fraud detection, Deep learning, Machine learning, Deep recursive neural network, Parallel model

Introduction

Every industry, including banking, education, and healthcare, has been modernized due to the growth of technology. Additionally, with the advent of communication technology, online transactions and payment methods are also undergoing modernization. As a result of this transformation, traditional currencies are being converted into digital currencies, and all financial transactions are increasingly conducted digitally. However, these transactions are not completely secure and remain vulnerable to various digital attacks, including fraud, anomalies, and privacy violations. Moreover, with the increase in transaction volumes, fraud in financial transactions is becoming more prevalent, leading to billions of dollars lost globally each year. Any suspicious activity on a network that deviates from normal behavior is referred to as an anomaly. In cybersecurity and digital financial exchanges, anomaly detection is employed to identify fraud and network intrusions. The primary goal of anomaly detection is to protect the network from illegal and fraudulent activities. In the financial sector, anomaly detection programs scrutinize suspicious activities to identify hackers and fraudulent users. However, all traditional anomaly detection methods are designed for centralized systems. Consequently, with the rise of cryptocurrencies such as Bitcoin, there is a need for improved anomaly detection methods that utilize blockchain technology [1]. Despite these advancements, instances of fraud continue to persist. With the increasing growth of the cryptocurrency market, Bitcoin has attracted considerable attention as one of the most famous and widely used cryptocurrencies. However, fraud and abuse in this market remain significant challenges. Detecting fraud in Bitcoin is crucial for maintaining the security, trust, and stability of the market. Bitcoin operates on a decentralized blockchain platform, where transactions are stored in a distributed ledger. The pseudonymous nature of Bitcoin transactions, the absence of a central authority, and the complex network of addresses pose significant challenges for fraud detection. Conventional fraud detection methods used in centralized systems may not be directly applicable to the blockchain platform due to the lack of centralized control and access to comprehensive transaction information [2]. Most existing fraud detection methods rely on rule-based systems or simplistic machine learning models that cannot adequately capture the complex and dynamic patterns associated with fraudulent activities. Deep learning techniques have demonstrated promising results in various sequence modeling tasks. The primary objective of this research is to leverage the capabilities of deep learning to capture the temporal dependencies and complex patterns in Bitcoin transactions, thereby enabling the development of a more accurate and efficient fraud detection system. To enhance performance in fraud detection, this research will focus on creating an effective model capable of identifying various types of fraudulent activities within the Bitcoin cryptocurrency [3]. Regarding scalability and real-time detection, the proposed fraud detection system must be able to handle the large number of transactions processed by the Bitcoin network while maintaining scalability and real-time detection capabilities. An essential challenge lies in utilizing crucial features to identify fraud in auto insurance. Feature selection techniques prioritize key features using criteria like chi-test, correlations, among others, selecting the top-ranking features as subsets. This process effectively eliminates irrelevant features [7]. Hence, it has been demonstrated that feature selection (FS) stands out as an effective strategy for enhancing model performance by mitigating the impact of noise and extraneous variables [8]. Feature selection aims to sift through surplus features and pinpoint the most fitting subset. Implementing feature selection within the dataset can diminish noise impact and lower computational costs during the modeling phase [9]. A critical strategy employed for optimizing parameter settings in XGBoost involves utilizing the feature selection technique [10]. Extreme Gradient Boosting (XGBoost) stands out as a state-of-the-art ensemble approach [11]. The XGBoost method assigns an importance score to each feature based on its contribution to critical decision-making processes within boosted decision trees, as proposed in [12]. Following the ranking of features based on their importance scores, an optimal subset is selected. To our knowledge, the exploration of XGBoost feature selection technique for fraud prediction remains uncharted territory. Continuing with the feature selection process, utilizing feature extraction can yield improved results directly from raw data while retaining essential information from the original dataset. This research will address the challenges associated with managing the vast amounts of data generated in the blockchain, optimizing computational efficiency, and achieving low-latency detection capabilities. This article aims to provide a powerful fraud detection system for Bitcoin on the blockchain using machine learning and deep learning algorithms. In particular, we will utilize recurrent neural networks, which have the ability to model and understand time patterns in time series data. In the first step, a dataset of Bitcoin transactions and related information will be collected. Next, we will apply recurrent neural networks to intelligently model this data and detect fraud patterns. Following this, we will implement various machine learning and deep learning algorithms on the dataset**.** Long Short-Term Memory **(LSTM)** is a type of recurrent neural network (RNN) designed to handle sequential data and address the vanishing gradient problem in traditional RNNs. It achieves this by utilizing memory cells and gating mechanisms (input, forget, and output gates) to selectively store, update, or discard information. LSTMs are widely used in applications like natural language processing, time-series forecasting, and speech recognition [13]. Gated Recurrent Unit **(GRU)** is a simplified version of Long Short-Term Memory (LSTM) networks, designed to model sequential data efficiently. It uses two gating mechanisms—reset and update gates—to control the flow of information without maintaining separate memory cells. GRUs are computationally less intensive than LSTMs and perform well in tasks like natural language processing and time-series prediction [14]. By employing sophisticated and advanced

techniques, these algorithms will identify patterns that indicate Bitcoin fraud. For example, they can detect anomalies related to sudden and unusual changes in transaction amounts, time patterns of transactions, and behaviors associated with suspicious addresses. Finally, based on the results of this fraud detection system, appropriate security measures will be recommended to prevent Bitcoin fraud and enhance trust in the market [15]. We assess the model's performance against two other studies using metrics like accuracy, precision, recall, and F1-score. The novel highlights of this paper are:

• Our proposed hybrid model represents a novel approach to predicting Bitcoin fraud in the blockchain environment, as it uses a combination of three distinct algorithms, each with a unique structure and architecture.

• This approach includes feature selection using the super-gradient boosting technique (XGboost), deep feature extraction, and classification and prediction using deep recurrent neural networks such as LSTM and GRU.

• In the proposed hybrid model of algorithms, which is a new and innovative approach to predicting Bitcoin fraud in the blockchain environment, aims to improve the accuracy and efficiency of detection and potentially helps in developing more effective fraud detection strategies.

• A detailed experimental analysis in terms of precision, accuracy, recall, and F1 score and confusion matrix to measure the performance of the proposed system.

The following sections of this paper are as follows:

- Section 2 provides an overview of relevant research on Bitcoin cryptocurrency fraud prediction in the blockchain context using machine learning techniques and deep recurrent neural networks.

- In Section 3, we describe the dataset in detail and outline our hybrid model architecture.

- Section 4 presents comprehensive empirical results of our model and provides an in-depth comparative analysis against alternative models.

- Finally, Section 5 concludes the findings of this research.

Literature Review

Shimal-Sh Tahir et al. in 2024, conducted a comprehensive study on detecting fraudulent transactions in cryptocurrency exchanges, with a primary focus on the Ethereum network. Utilizing various machine learning techniques and ensemble methods, including the hard voting ensemble model, which achieved an impressive accuracy of 99%, their objective was to effectively identify suspicious transactions while maintaining high precision and accuracy. Moreover, they emphasized the significance of explainable artificial intelligence (XAI) to enhance transparency, trust, and accountability in AI-based fraud detection systems. Their research contributes to the development of reliable and interpretable models that can significantly improve the security and integrity of the cryptocurrency ecosystem [16]. In 2023, Rosalyn Ogundokun et al. conducted a study on blockchain and its infrastructure. This study proposed the use of deep learning methods, including bidirectional short-term memory (BiLSTM) and convolutional neural networks (CNN), to detect phishing attacks in a blockchain transaction network. These methods were evaluated on a dataset comprising malicious addresses from blockchain blacklists and benign addresses from whitelists, achieving an accuracy of 99.72%. Recent advancements in blockchain and wireless communication infrastructures have paved the way for developing blockchain-based systems that safeguard data integrity and enable secure information sharing. Despite these advancements, concerns regarding security and privacy continue to hinder the widespread adoption of blockchain technology, especially when sharing sensitive data. Specific security threats against blockchains, such as data poisoning attacks, privacy leaks, and single points of failure, must be addressed to develop efficient IT infrastructures supported by blockchain technology[17]. In 2023, Q. Omer et al. presented a study proposing an ensemble learning approach for detecting fraudulent cryptocurrency transactions by integrating two deep learning methods: convolutional neural networks (CNNs) and long short-term memory (LSTM) networks. The two algorithms were compared in terms of accuracy and training/testing dataset losses. Additionally, a 10-fold cross-validation approach was employed to evaluate the proposed method. The evaluation results demonstrated that the ensemble approach, incorporating deep recurrent LSTM networks, achieved a notable accuracy of 96.4%, outperforming other approaches [18]. In 2023, Ting Wen et al. introduced a model

designed to address the financial security threats in blockchain systems. Their study proposed a hybrid deep neural network model for identifying phishing fraud accounts, referred to as the LSTM-FCN-BP phishing fraud account detection model. The model's efficacy was validated on the Ethereum network. The LBPS model combines a backpropagation (BP) neural network to capture implicit relationships between features extracted from transaction records and an LSTM-FCN (fully convolutional network) to extract temporal features from the complete transaction history of a target account. Experimental results showed that the selected features effectively identified phishing fraud accounts. Furthermore, the LBPS model outperformed existing methods and baseline models, achieving a harmonic mean accuracy of 97.86% [19]. In 2023 Swapna Sidam Sethi et al. presented a groundbreaking paper bridging artificial intelligence (AI) and blockchain technologies. In the context of anomaly detection, this study highlighted the significance of blockchain technology and its applications in the financial sector. By collecting Bitcoin blockchain transaction data, they employed unsupervised machine learning algorithms to detect fraudulent transactions. Although various AI algorithms were proposed for anomaly detection, none consistently outperformed the others. Their study applied a range of unsupervised machine learning techniques, including Isolation Forest, cluster-based Local Outlier Factor, deep autoencoder networks, and ensemble approaches, to identify potentially fraudulent transactions. The paper emphasized the synergy between blockchain technology and anomaly detection in financial security, offering a comprehensive perspective on modern fraud detection methodologies [20]. In 2022 Fatemeh Salahuddin et al. introduced a novel method for detecting phishing attacks using machine learning. This approach utilized an artificial neural network (ANN) to identify suspicious features in emails. The researchers trained the ANN on a dataset of 4,000 phishing and legitimate emails. The results demonstrated that this method could detect phishing attacks with 95% accuracy, showcasing the potential of machine learning as an effective tool for combating phishing. The proposed method can enhance the security of both users and organizations by mitigating the risks posed by phishing attacks [21]. In 2022 Rubiya Moshar Aziz et al. proposed a Light Gradient Boosting Machine (LightGBM)-based approach for accurate detection of fraudulent transactions. They compared this method with other models such as Random Forests and Multilayer Perceptrons, leveraging machine learning and soft computing algorithms to classify fraud detection datasets from Ethereum with limited features. Comparative analysis revealed that LightGBM and Extreme Gradient Boosting (XGBoost) algorithms achieved the highest accuracy. Further optimization of LightGBM using hyperparameter tuning yielded an accuracy of 99.03%, surpassing other models and proving its effectiveness for Ethereum fraud detection scenarios [22]. In 2022 Lin Liu et al. developed a heterogeneous graph transformer network for anomaly detection in smart contracts to identify financial fraud on the Ethereum platform. Their model first extracted features to construct a heterogeneous information network (HIN) for smart contracts and then utilized a meta-path-driven relational matrix as input for the network. Node embeddings were subsequently applied for classification tasks. The classification results showed superior performance compared to traditional models, with low standard deviations, demonstrating the model's effectiveness and stability. This anomaly detection method for smart contracts effectively mitigates hidden security risks such as financial fraud, illegal financing, and money laundering. Ethereum, as the largest platform for smart contracts, requires robust fraud detection methods due to the complexity and sheer volume of smart contract data. The study underscores the importance of high-level feature extraction and efficient detection of anomalous contracts to enhance financial security[23].. In 2022 Tahreem Ashfaq et al. proposed an efficient blockchain-based fraud detection mechanism using machine learning. They developed a secure fraud detection model leveraging machine learning and blockchain technologies. Two machine learning algorithms, XGBoost and Random Forest, were employed to classify transactions. The system utilized learning techniques to train models on datasets containing patterns of fraudulent and legitimate transactions. The trained models then predicted new incoming transactions, ensuring robust and efficient fraud detection [24]. In 2020, Francisco Saichitano and colleagues developed an anomaly detection system using deep learning for monitoring blockchain activities, proving effective in identifying reported attacks on the Ethereum Classic network. This innovative approach provides a comprehensive solution for enhancing blockchain transaction security. Despite the widespread use of blockchain technology for improving data privacy and system security, vulnerabilities such as the successful 51% attack on Ethereum Classic in January 2019 highlight the ongoing risk of cyber attacks in blockchain systems [25].

Material and Method

Figure 1 shows the architecture of our hybrid model in 6 steps:

A Data Collection

In the first step, a Bitcoin dataset is collected from an open repository available on the Kaggle website[1].

[1] https://www.kaggle.com/datasets/ellipticco/elliptic-data-set

B. Data Preprocessing and Normalization

This step involves preprocessing and normalizing the data. Missing data is either imputed or removed. Subsequently, using standardization and normalization techniques, all features of the Bitcoin dataset, except for the class label feature, are processed to transform their values into a numerical range of either [0, 1] or [-1, 1).

C. Feature Selection

Important features influencing fraud detection are selected using feature selection techniques and the Extreme Gradient Boosting (XGBoost) algorithm.

D. Deep Feature Extraction and Transaction Pattern Classification and Prediction Using Recurrent Neural Networks in Parallel Model

The Parallel Model combines two sequential architectures, GRU (Gated Recurrent Unit) and LSTM (Long Short-Term Memory), to extract complementary features from input time-series data. Initially, the input data passes through three stacked GRU layers (GRU_Layer_1, GRU_Layer_2, GRU_Layer_3), each with dropout and batch normalization for regularization and stability. The outputs from these GRU layers are fed into separate LSTM layers (LSTM_Layer_1, LSTM_Layer_2, LSTM_Layer_3), enabling the model to capture both short-term and long-term dependencies in the data. The resulting outputs are further processed through Dense_Layer_1 and Dense_Layer_2, which use LeakyReLU activation for nonlinearity. These layers, along with the final LSTM output (LSTM_Layer_3), are concatenated in the Concatenation_Layer to combine features extracted from all branches. Finally, the merged features are passed to the Output_Layer, which uses a softmax activation function to produce class probabilities, making this architecture a robust combination of GRU and LSTM models for sequential data tasks.

E. Model Performance Evaluation

The model's performance is assessed using evaluation metrics such as accuracy, precision, recall, and a confusion matrix

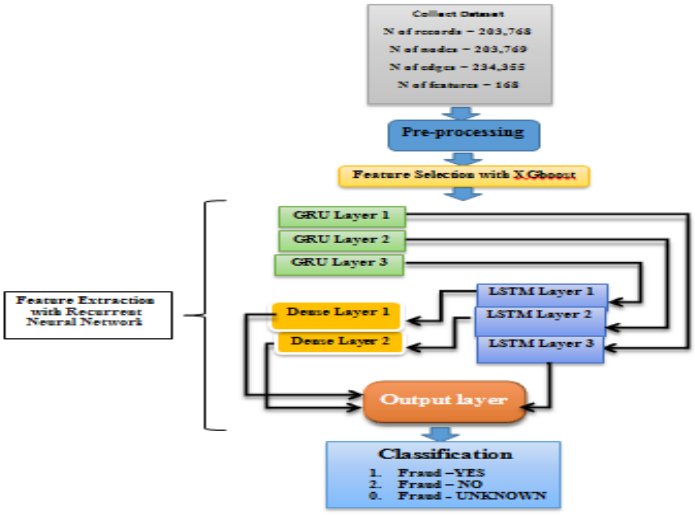

Fig (1) The architecture of our proposed hybrid mode

Experimental results

In this section, we examine the experimental results of the proposed model and compare the proposed hybrid model with other models in the previous papers

A. Dataset

To evaluate our methodology, we used as an open repository dataset. According to Figure 2, the dataset used includes 166 features associated with each node. Among these, 94 features represent local information about the transaction, such as the number of inputs/outputs, transaction fees, output volume, and aggregated figures, including

the average Bitcoin received and spent by inputs/outputs, as well as the average number of input/output transactions linked to the inputs/outputs. The remaining 72 features are aggregated features derived using information from neighboring transactions in both directions. These features include the maximum, minimum, standard deviation, and correlation coefficients of neighboring transactions for the same informational data (e.g., number of inputs/outputs, transaction fees, etc.).

B. Results of XGboost-GRU-LSTM model

The bitcoin fraud dataset contains 203769 records, of which 4545 records belong to the fraud class and 42019 records belong to the non-fraud class and 157205 records belong to unknown class. One of the key techniques in data transformation methods is data normalization or standardization. Transforming variable types in the dataset can lead to significantly different outcomes, which can enhance the accuracy and efficiency of algorithms, resulting in higher-quality results. This step was performed using the Min-Max Scaler normalization library.

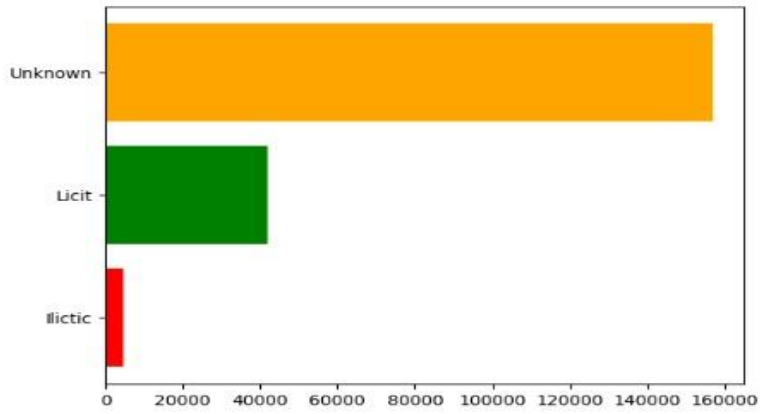

Fig (2) Plot of classes in dataset

To identify the important features of the Bitcoin dataset, the XGBoost Classifier was utilized. According to the report and the results obtained, as shown in Figure 3, the most significant features were transaction-related attributes. These features play a crucial role in detecting fraud within the Bitcoin dataset, influencing the outcomes significantly.

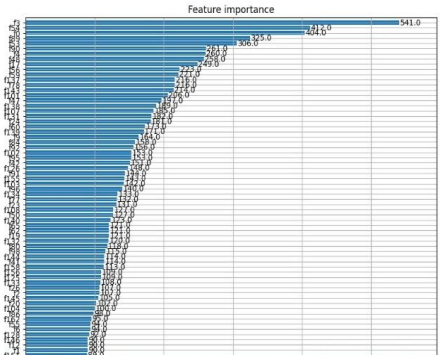

Fig (3) Plot of ten importance features

The Policy Transaction feature 47 is one of the most important features with a score of 0.19331. We divide the dataset into three sets to evaluate and test the performance of the hybrid model. The training, validation and testing sets contain 80%, 10% and 10% of the dataset. According to Figure 4 using GRU model with 64, 128, and 256 recurrent neurons, we extracted deep features from the dataset. The total number of parameters for the extracted features amounted to 385,600.

Model: "Parallel GRU-LSTM Model"

Layer (type)	Output Shape	Param #	Connected to
Input_Layer (InputLayer)	(None, 30, 1)	0	–
GRU_Layer_1 (GRU)	(None, 30, 64)	12,864	Input_Layer[0][0]
batch_normalization (BatchNormalization)	(None, 30, 64)	256	GRU_Layer_1[0][0]
dropout (Dropout)	(None, 30, 64)	0	batch_normalization[0…
GRU_Layer_2 (GRU)	(None, 30, 128)	74,496	dropout[0][0]
batch_normalization_1 (BatchNormalization)	(None, 30, 128)	512	GRU_Layer_2[0][0]
dropout_1 (Dropout)	(None, 30, 128)	0	batch_normalization_1…
GRU_Layer_3 (GRU)	(None, 30, 256)	296,448	dropout_1[0][0]
batch_normalization_2 (BatchNormalization)	(None, 30, 256)	1,024	GRU_Layer_3[0][0]
dropout_2 (Dropout)	(None, 30, 256)	0	batch_normalization_2…
LSTM_Layer_1 (LSTM)	(None, 256)	525,312	dropout_2[0][0]
LSTM_Layer_2 (LSTM)	(None, 128)	131,584	dropout_1[0][0]
batch_normalization_6 (BatchNormalization)	(None, 256)	1,024	LSTM_Layer_1[0][0]
batch_normalization_7 (BatchNormalization)	(None, 128)	512	LSTM_Layer_2[0][0]
dropout_8 (Dropout)	(None, 256)	0	batch_normalization_6…

Fig (4) Deep feature extraction based on GRU **architecture**

The outputs generated by these GRU layers are then passed to three separate LSTM layers—LSTM_Layer_1, LSTM_Layer_2, and LSTM_Layer_3—allowing the model to learn both short-term and long-term dependencies within the data. Subsequently, the outputs from the LSTM layers are fed into two fully connected layers, Dense_Layer_1 and Dense_Layer_2. Alongside these layers, the final LSTM output from LSTM_Layer_3 is also included in the feature extraction process. The extracted features from all branches are concatenated in the Concatenation_Layer, integrating the learned representations into a unified feature set. Finally, the merged features are processed by the Output_Layer, which employs a softmax activation function to generate class probabilities, making the model highly effective for sequential data classification tasks. The total number of parameters for the extracted features amounted to 1111043.

dropout_9 (Dropout)	(None, 128)	0	batch_normalization_7…
Dense_Layer_1 (Dense)	(None, 64)	16,448	dropout_8[0][0]
Dense_Layer_2 (Dense)	(None, 128)	16,512	dropout_9[0][0]
LSTM_Layer_3 (LSTM)	(None, 64)	33,024	dropout[0][0]
leaky_re_lu_2 (LeakyReLU)	(None, 64)	0	Dense_Layer_1[0][0]
leaky_re_lu_3 (LeakyReLU)	(None, 128)	0	Dense_Layer_2[0][0]
batch_normalization_8 (BatchNormalization)	(None, 64)	256	LSTM_Layer_3[0][0]
dropout_11 (Dropout)	(None, 64)	0	leaky_re_lu_2[0][0]
dropout_12 (Dropout)	(None, 128)	0	leaky_re_lu_3[0][0]
dropout_10 (Dropout)	(None, 64)	0	batch_normalization_8…
Concatenation_Layer (Concatenate)	(None, 256)	0	dropout_11[0][0], dropout_12[0][0], dropout_10[0][0]
Output_Layer (Dense)	(None, 3)	771	Concatenation_Layer[0…

Total params: 1,111,843 (4.24 MB)
Trainable params: 1,109,251 (4.23 MB)
Non-trainable params: 1,792 (7.00 KB)

Fig (5) Deep feature extraction based on Parallel model architecture

We set the number of training epochs to 100 and the batch size for data injection into the network to 64. According to the results obtained from the parallel model, the accuracy of the training data was 92.81%, and the accuracy of the testing data was 92.67%. These results indicate that the model does not suffer from overfitting. Figure 6 shows the confusion matrix plot of the proposed hybrid model.

TABLE 1- THE PERFORMANCE OF THE PROPOSED MODEL

Class	Model's performance evaluation		
	F1-Score	Precision	Recall
Fraud	92.14%	86.35%	99.18%
Non-Fraud	91.03%	90.82%	91.25%
Unknown	97.57%	97.80%	97.34%

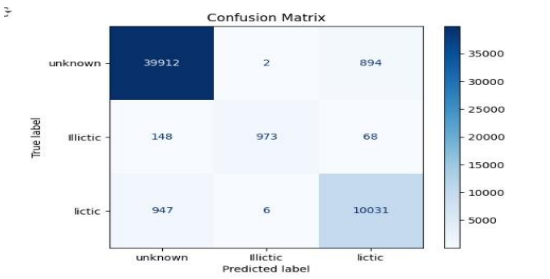

Fig (6) The Confusion matrix proposed hybrid model

According to Figure 6, the error rate decreases significantly after 100 training epochs, while the sizes of the training and evaluation datasets continue to decrease sharply. The lines on the graph are closely spaced, indicating that the model has not overfitted and that it exhibits generalization. In Figure 7, we present the evaluation of the model on the training datasets, where we obtained accuracy and cost function values over the course of 100 epochs. The results show that the model approaches an accuracy of 95%, with the lines on the graph remaining closely spaced, suggesting that the model is not overfitting.

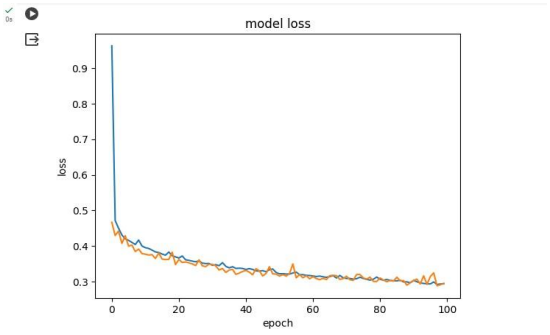

Fig (7) The plot of the cost function for the training dataset

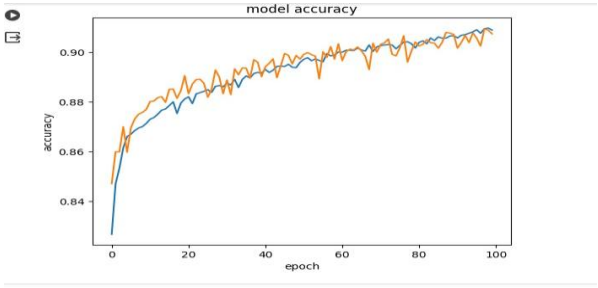

Fig (8) The plot of accuracy for the training dataset

CONCLUSION

In this paper, we proposed a hybrid model using 203769 datasets for Fraud detection in Bitcoin cryptocurrency on the Blockchain platform. The data used is from an open source, which includes 4545 cases of fraud and 42019 cases of non-fraud and 157205 cases of unknown. We used the Min-Max scaler Normalization method to normalize and standardize the data. We used a hybrid model of machine learning and deep learning to predict Bitcoin cryptocurrency fraud on the Blockchain platform. In this model, we used the XGboost algorithm to select important features. Then, we used a parallel model using deep recurrent neural network with GRU and LSTM to extract deep features and make predictions. The test results on the Bitcoin cryptocurrency fraud dataset are 92.67% accurate, 92.66% precision, 95.92% recall and 93.58% F1 score. The results obtained from our proposed hybrid model show that it can be used as an intelligent tool to detect fraud in Bitcoin cryptocurrency on the Blockchain platform in cryptocurrency market.

Acknowledgment

This research was supported by Rouzbahan Institute of Higher Education. We thank our colleagues from Dr. Behnam Barzegar who provided insight and expertise that greatly assisted the research, although they may not agree with all of the conclusions of this paper.

References

[1] Podgorelec, B., Turkanović, M., & Karakatič, S. (2019). A machine learning-based method for automated blockchain transaction signing including personalized anomaly detection. Sensors, 20(1), 147.

[2] Jung, E., Le Tilly, M., Gehani, A., & Ge, Y. (2019, July). Data mining-based ethereum fraud detection. In 2019 IEEE international conference on blockchain (Blockchain) (pp. 266-273). IEEE.

[3] Kamps, J., Trozze, A., & Kleinberg, B. (2022). Cryptocurrencies:: Boons and curses for fraud prevention. In A Fresh Look at Fraud (pp. 192-219). Routledge.

[4] Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review, 40, 100402.

[5] Pham, T., & Lee, S. (2016). Anomaly detection in the bitcoin system-a network perspective. arXiv preprint arXiv:1611.03942.

[6] Zhang, R., Zhang, G., Liu, L., Wang, C., & Wan, S. (2020). Anomaly detection in bitcoin information networks with multi-constrained meta path. Journal of Systems Architecture, 110, 101829.

[7] Signorini, M., Pontecorvi, M., Kanoun, W., & Di Pietro, R. (2018, July). Advise: anomaly detection tool for blockchain systems. In 2018 IEEE World Congress on Services (SERVICES) (pp. 65-66). IEEE.

[8] Kamišalić, A., Kramberger, R., & Fister Jr, I. (2021). Synergy of blockchain technology and data mining techniques for anomaly detection. Applied Sciences, 11(17), 7987.

[9] Laiche, A., Deep Learning on FPGA (Simulation and Implementation). UNIVERSITY OF OUARGLA.

[10] [12]VanRossum, G. and F.L. Drake, The python language reference. Vol. 561. 2010 : python Software Foundation Amsterdam, Netherlands.

[11] Zhu, M., Ye, K., Wang, Y., & Xu, C. Z. (2018). A deep learning approach for network anomaly detection based on AMF-LSTM. In Network and Parallel Computing: 15th IFIP WG 10.3 International Conference, NPC 2018, Muroran, Japan, November 29–December 1, 2018, Proceedings 15 (pp. 137-141). Springer International Publishing

[12] Schueffel, P., Groeneweg, N., & Baldegger, R. (2019). The Crypto Encyclopedia: Coins, tokens and digital assets from A to Z.Kkkh

[13] Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of economic Perspectives, 29(2), 213-238.

[14] Chen, Y., et al., Deep feature extraction and classification of hyperspectral images based on convolutional neural networks. IEEE transactions on geoscience and remote sensing, 2016. 54(10): p. 6232-6251.

[15] Hasan Pranto, T., Hasib, K. T. A. M., Rahman, T., Bahalul Haque, A. K. M., Najmul Islam, A. K. M., & Rahman, R. M. (2022). Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach. arXiv e-prints, arXiv-2210.

[16] Taher, S. S., Ameen, S. Y., & Ahmed, J. A. (2024). Advanced Fraud Detection in Blockchain Transactions: An Ensemble Learning and Explainable AI Approach. Engineering, Technology & Applied Science Research, 14(1), 12822-12830.

[17] Ogundokun, R. O., Arowolo, M. O., Damaševičius, R., & Misra, S. (2023, May). Phishing Detection in Blockchain Transaction Networks Using Ensemble Learning. In Telecom (Vol. 4, No. 2, pp. 279-297). MDPI.

[18] Umer, Q., Li, J. W., Ashraf, M. R., Bashir, R. N., & Ghous, H. (2023). Ensemble Deep Learning Based Prediction of Fraudulent Cryptocurrency Transactions. IEEE Access.

[19] Wen, T., Xiao, Y., Wang, A., & Wang, H. (2023). A novel hybrid feature fusion model for detecting phishing scam on Ethereum using deep neural network. Expert Systems with Applications, 211, 118463.

[20] Siddamsetti, S., & Srivenkatesh, M. (2024). Deep Blockchain Approach for Anomaly Detection in the Bitcoin Network. International Journal of Intelligent Systems and Applications in Engineering, 12(1), 581-595.

[21] Salahdine, F., El Mrabet, Z., & Kaabouch, N. (2021, December). Phishing Attacks Detection A Machine Learning-Based Approach. In 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0250-0255). IEEE.

[22] Aziz, R. M., Baluch, M. F., Patel, S., & Ganie, A. H. (2022). LGBM: a machine learning approach for Ethereum fraud detection. International Journal of Information Technology, 14(7), 3321-3331.

[23] Liu, L., Tsai, W. T., Bhuiyan, M. Z. A., Peng, H., & Liu, M. (2022). Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum. Future Generation Computer Systems, 128, 158-166.

[24] Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. Sensors, 22(19), 7162.

[25] Yazdinejad, A., HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Srivastava, G., & Chen, M. Y. (2020). Cryptocurrency malware hunting: A deep recurrent neural network approach. Applied Soft Computing, 96, 106630.