

Detecting Anomalous Transaction Patterns on Cryptocurrency Exchanges using On-Chain Data

M.J. Jeyasheela Rakkini¹, Rahul Shridhar.V² and Kishore Kumar³

¹⁻³Sastra Deemed University/School of Computing, Thanjavur, India

Email: jeyasheelarakkini@cse.sastra.ac.in, {125003489,125003488}@sastra.ac.in

Abstract—Exchanges for cryptocurrencies are essential to the cryptocurrency market. However, while offering user services, certain exchanges are suspected of engaging in various strange or malevolent activities, including money laundering and wash trading. Furthermore, it has been noted that these actions frequently result in an unusual rise in the transaction amount. Determining whether and when the anomalous transaction amount happens in the exchange is therefore a topic worthy of investigation. This study gathers a comprehensive dataset of exchanges, and then it does a correlation analysis to identify the key variables influencing the transaction volume of various exchanges. Next, using deep learning, a prediction model of how different parameters affect the transaction amount is obtained. To establish a foundation for the identification of anomalous transaction amounts, the difference between the anticipated and actual transaction amounts is computed. Ultimately, a case study on the detection results reveals that some anomalous transaction amounts are connected to industry events and policy changes, while the remaining quantities are thought to be connected to illicit activity. The root mean square error ranges from 0.07 to 0.7, the mean absolute error ranges from 0.02 to 0.09 and the mean absolute percentage error ranges from 0.3 to 0.5 for all the five crypto exchanges for our prediction if anomalous transaction by deep learning models.

Keywords— Blockchain, Cryptocurrency, Exchange Anomaly detection.

I. INTRODUCTION

Blockchain is a technology that possesses immutability, anonymity, and decentralization. It has been extensively utilized in several industries recently, including risk management, financial services, and digital currencies. Cryptocurrency is one of the applications that has received a lot of interest. Since blockchain is the underlying technology of cryptocurrencies, its emergence has led to a significant increase in their popularity and development in recent years. After Bitcoin, Ethereum is the second-biggest digital currency trading platform and the largest blockchain that facilitates smart contracts. On the one hand, the Ethereum platform has seen significant use in the financial and economic spheres and has grown to become a well-known, developing investment market. However, as a developing investment sector, many illicit transactions are bound to occur. Cryptocurrency exchanges offer consumers services for buying, selling, and trading cryptocurrency, much like traditional finance [1]. There are two types of exchanges: centralized and decentralized. Since centralized exchanges now control a large portion of the cryptocurrency industry, this paper will concentrate on the centralized concentrated exchange scenario. The concentrated exchange in centralized exchanges will trade only specific asset class or a group of assets.

The digital assets that are traded in centralized exchange is (CEX) is cryptocurrencies, tokens, non-fungible tokens and derivatives. CEX provide secure trading but it can suffer from anomalous trading activities. Market manipulation, Pump and Dump schemes, Wash trading, insider trading, spoofing and front running are the various anomalous trading activities. Mt. Gox world's largest bitcoin exchange suffered bankruptcy owing to the theft of 850,000 bitcoins from it in 2014 and a rehabilitation plan was arranged in late 2021[2]. The transaction history of Mt.Gox was taken and it was classified in to three different accounts such as low account, high account and extreme high account. Graphs were constructed for low account, extreme high account and extreme low account. The graphs were further fine-tuned as daily snapshots and matrices were constructed out of it. Singular value decomposition was conducted on these matrices and this helps in identifying transactions with abnormal values. Additionally, some exchanges manipulate the market by inflating trading volumes. The "Pump and Dumps scheme" (P&D) is a common example of market manipulation fraud [3]. Price gouging raises a cryptocurrency's value quickly by requiring all buyers to purchase it at the same time. Consequently, a high volume of people buying currency at once, indicating an unusual spike in the transaction amount, is required for P&D behavior to occur. It is crucial and urgent to determine whether and when the anomalous transaction amount occurs on the exchange because when the aforementioned behaviours take place there, the transfer of a significant amount of cryptocurrency would reflect abnormal variations in the transaction amount. It is the duty of exchanges as well as the expectations of investors to identify anomalous transaction amounts, safeguard investor interests, and establish a fair trading environment. However, no research has yet been conducted to provide a comprehensive and reasonable framework for the identification of irregular transaction amounts on crypto exchanges, nor has any research been conducted to compile a comprehensive dataset containing the crypto exchange transaction amount and other relevant data.

The main contribution of this paper is

A complete dataset of cryptocurrency exchanges is obtained from the top five exchanges on CoinMarketCap and this research uses a deep learning prediction model with an added attention mechanism to analyze different transactions from the perspective of time series prediction. Abnormal transaction amount and the time of abnormal transaction amount are detected using this deep learning prediction model.

The method consists of the following analysis.

- From each of the exchange dataset determine the important factors of each exchange through pearson and spearman rank correlation analysis.
- Conduct experiments with important factors as well as unimportant factors. We select the core factors affecting the transaction amount for each exchange using the threshold (τ)
- The threshold (τ) for determining strong or weak correlation in Binance, Kucoin, Kraken and Coinbase, is 0.4 and for Huobi, τ is 0.3.
- Use different deep learning models to analyze different transactions from the perspective of time series prediction

II. LITERATURE SURVEY

The survey of blockchain anomaly detection systems with the identification of universal detection methods and specific detection methods with 8 sub-classes is devised in [4]. In each subclass, the research is listed, categorized and compared for the detection of anomalous transactions in Bitcoin blockchain. This study [5] identifies suspicious transaction from Binance, an open-source cryptocurrency trading platform, by defining and detecting cryptocurrency wallets. By taking the metadata of 38,526 wallets from etherscan.io, the investigation of transactions is done. This study also performed an unsupervised learning model, namely the expectation maximization (EM) algorithm. Based on the features engineered from unsupervised learning, anomaly detection using Random Forest (RF) was devised. However, Random Forests in anomaly detection may lack interpretability, struggle with imbalanced data, and require careful parameter tuning, while also being computationally expensive for large datasets. The study [6] uses traditional machine learning methods like One-Class Support Vector Machine and Isolation Forest. This proves ineffective in detecting anomalies in Ethereum transactions due to their inability to capture the inter-node or account relationship information present in these transactions. Ethereum transactions can be accurately depicted using an attributed graph format, where nodes and edges encapsulate the interdependencies. But One-Class Support Vector Machine and Isolation Forest can struggle with high-dimensional data. The potential of Graph Convolutional Networks (GCN) and Graph Attention Networks (GAT) as promising solutions for Anti-Money Laundering and they combat the financing of Terrorism (AML/CFT) tasks is shown in [7]. Notably, GCN outperforms traditional methods in this context,

while GAT is employed for the first time to detect anomalies in Bitcoin transactions. However, GAT requires significant computational resources for training, limiting their scalability in anomaly detection tasks. A novel model for detecting anomalies in Bitcoin electronic transactions is shown in [8]. This approach incorporates two machine learning algorithms: One-Class Support Vector Machines (OCSVM) for outlier detection, and K-Means for clustering similar outliers with matching types of anomalies. Since some crypto accounts exhibit illicit behavior, the account classification of the crypto addresses(accounts) is shown in [9]. The accounts are shown as a node, which can be augmented with more information and these nodes form a graph neural network. Each node that represents an account can be audited for transaction behavior. Anomaly detection for suspicious users and transactions is done in [10]. The bitcoin transaction network generates two graphs. The law of power degree, local power outlier detection factor method and k means the cluster is executed on the graphs. Isolation forest [11] is developed to classify cryptocurrency transactions that are legitimate or fraudulent. Each transaction has an anomaly score which depends on the isolation forest tree length. To detect anomalies in Bitcoin and Ethereum transaction networks, GPU-accelerated machine learning models that include support vector machines, random forest and logistic regression are carried out on the metadata of Bitcoin and Ethereum transactions. [12]. Two distinct machine learning models are used on two prevalent account types: externally owned accounts (EOA) and smart contract accounts [13]. Malicious activities are used to detect anomalies in cryptocurrency transactions. Anomaly detection also involves the detection of Ponzi schemes, tax evasion using pseudo-anonymous transactions and multiple identities that accumulate funds. Investigation of the viability of employing anomaly detection and active learning algorithm to find novel fraudulent patterns in cryptocurrency transactions is done in [14]. To effectively detect threats, transaction record details must be thoroughly examined, and adversaries may use this information to launch de-anonymization and model interference assaults. Therefore, while creating an anomaly detection system for Bitcoin transactions, privacy preservation must come first. There are very few publications on anomaly detection at the level of the exchange transaction amount, and this paper fills the gap of this research.

III. EXISTING WORK

A. Data Collection

Etherscan, an Ethereum community-operated platform, offers a specialized API for accessing public Ethereum transaction records. The data has been collected from five top crypto exchanges such as Binance, Coinbase, Huobi, Kraken and Kucoin. One of its features, the Label Word Cloud, categorizes crypto addresses with labels such as exchange, phishing, and gambling crypto addresses. Our process involves consolidating transaction information for accounts associated with the same exchange and aggregating data based on timestamps. For instance, transactions occurring on the same day across various account addresses are treated as transactions for that exchange. The attributes in the dataset are timestamp, transaction amount, transaction count, active addresses, average transaction value, account balances, gas fees, market capitalization, liquidity metrics, exchange identifier, token type, price at transaction time, user behaviour metrics and network metrics. The following steps are carried out: correlation analysis with the spearman correlation coefficient, Pearson correlation coefficient and abnormal transaction detection with deep learning models for the time series of data of crypto exchanges.

B. Correlation Analysis

Spearman correlation coefficient (1) and Pearson correlation coefficient (2) are used to explore the impact of the exchange's on-chain metrics on its transaction amount. We perform correlation analysis on various factors and transaction amounts.

C. Pearson Correlation Coefficient

Where $\bar{X}$ - Mean value of X

$\bar{Y}$ - Mean values of Y

$$r = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2 \sum_{i=1}^n (y_i - \bar{y})^2}} \quad (1)$$

Spearman rank correlation coefficient

Where n – number of elements in each dataset

d- difference between corresponding values of x and y respectively

$$\rho = 1 - \frac{6 \sum d_i^2}{n(n^2-1)} \quad d_i = x_i - y_i \quad -(2)$$

The study's objective is to determine which on-chain metrics have a substantial impact on transaction amounts by computing the correlation coefficients.

Metrics that are important in forecasting regular and anomalous transactions include, for instance, the number of unique active addresses, transaction counts (frequency), transaction volume, and fees, which may exhibit substantial correlations with transaction quantities.

Through correlation analysis, the factors identified are transaction count, account balance and unique addresses. The characteristics that are chosen for the deep learning models (such as the LSTM_attention model, GRU attention) are influenced by the findings of the correlation analysis. There are 18 onchain metrics considered for correlation which are listed below,

TABLE I. ON CHAIN METRICS OF ETHEREUM TRANSACTIONS

1.eth_account_balance	The account balance in Ether.
2.usd_eth	The price of Ether in US Dollars.
3.historic_usd_val	The account balance expressed in US Dollars.
4.transaction_count_total	The total number of transactions.
5.transaction_count_sent	The number of transactions for sending Ether.
6.transaction_count_recv	The number of transactions for receiving Ether.
7.fee_spent_eth	The fee cost incurred for sending transactions
8.fee_used_eth	The fee cost incurred for receiving transactions.
9.token_transfers	The number of tokens transferred.
10.outbound_transfers	The number of tokens transferred outbound.
11.inbound_transfers	The number of tokens transferred inbound.
12.unique_address_sent	The number of unique addresses sending tokens.
13.unique_address_recv	The number of unique addresses receiving tokens.
14.token_contracts_count	The number of contract addresses involved.
15.unique_outgoing_address	The number of unique addresses for outgoing transactions.
16.unique_incoming_address	The number of unique addresses for incoming transactions.
17.ether_sent_out	The amount of Ether sent out.
18.ether_recv_in	The amount of Ether received in

The metrics are crucial for performing correlation analysis to identify the factors significantly influencing transaction amounts on different exchanges.

C. Abnormal transaction detection

The first step in our LSTM is to decide what information we're going to throw away from the cell state. The sigmoid function makes the decision by taking the previous output "h" and input feature "x" along with bias "b" as shown in (3).

$$i_t = \sigma(W_i [h_{t-1}, x_t] + b_i) \quad -(3)$$

The next step is to decide what new information we're going to store in the cell state. This has two parts. First, a sigmoid layer called the "input gate layer" decides which values we'll update. Next, a tanh layer creates a vector of new candidate values, C_t , that could be added to the state as shown in (4).

$$c_t = \tanh(W_i [h_{t-1}, x_t] + b_i) \quad -(4)$$

$$f_t = \sigma(W_f [h_{t-1}, x_f] + b_f) \quad -(5)$$

The forget gate is shown in (5). In the next step, we'll combine these two to create an update to the state.

$$C_t = f_t * c_{t-1} + i_t * \tilde{c}_t \quad -(6)$$

This is the new candidate value C_t , scaled by how much we decided to update each state value as shown in (6). The cell state is put through tanh (to push the values to be between $[-1,1]$) and multiplied by the output of the sigmoid gate, so that we only output the parts we decided to. The detection of abnormal transactions leverages an LSTM model.

GRU model with an attention mechanism to analyze transaction data effectively, identify significant deviations, and enhance the overall security and reliability of the exchange.

IV. PROPOSED SYSTEM

GRU uses a simpler gating mechanism with fewer components (reset and update gates), but it also benefits from more hidden units for capturing sequence dependencies. While the GRU is simpler, increasing hidden units can still allow it to learn more complex patterns. The number of hidden units is in the range from [32, 64, 128, 256]. The batch size is in the range from [32, 64, 128]. The sequence length is in the range from [5, 10, 15, 20]. The GRU consists of two main gates update gate and reset gate. The input sequence X consists of a sequence of a data with each time step containing one or more features. The reset gate (r) controls how much of past information to forget. Update gate (z) decides how much of the previous hidden state should be retained and how much of the previous hidden state should be incorporated. Candidate hidden state ($\tilde{h}$) is calculated based on the current input and previous hidden state and the reset gate influences it. Final hidden state (h) is the combination of the previous hidden state and candidate hidden state controlled by update gate.

Given an input sequence $X=(x_1, x_2, \dots, x_t)$ the GRU processes the data as follows:

Reset gate

$$r_t = \sigma(W_r x_t + U_r h_{t-1} + b_r) \quad (7)$$

Update Gate:

$$z_t = \sigma(W_z x_t + U_z h_{t-1} + b_z) \quad (8)$$

Candidate Hidden State:

$$\tilde{h}_t = \tanh(W_h x_t + U_h (r_t \cdot h_{t-1}) + b_h) \quad (9)$$

Final Hidden State:

$$h_t = (1 - z_t) \cdot h_{t-1} + z_t \cdot \tilde{h}_t \quad (10)$$

Where W_r, W_z, W_h are weight matrices for the reset gate, update gate, and candidate hidden state, respectively. U_r, U_z, U_h are weight matrices for the previous hidden state. b_r, b_z, b_h are bias terms. σ is the sigmoid activation function. $\tanh$ is the hyperbolic tangent activation function. h_t is the hidden state at time step t . Here equations (7), (8), (9) and (10) are the functions for reset, update, candidate hidden state and final hidden state.

V. RESULTS

Based on the performance comparison presented in Table 3, the Gated Recurrent Unit (GRU) demonstrates the lowest error values root mean square error (RMSE), mean absolute error (MAE) and mean absolute percentage error (MAPE) across most exchanges, particularly in Binance, Kraken, and Coinbase. While LSTM with Attention occasionally outperforms GRU and LSTM in MAPE, its performance is inconsistent across all metrics. LSTM shows competitive results for Huobi and Kucoin but is largely surpassed by GRU. Overall, GRU stands out as the most balanced model, achieving lower error rates across multiple metrics and exchanges, though there are instances where LSTM performs better in certain areas. MSE is used to compare the fitting performance of different models when predicting transaction amounts for different exchanges. The lower the RMSE value, the better the performance. MAPE gives the size of the error in percentage terms. Lower MAPE indicates the correct selection of parameters. The lower mae, rmse, and mape for the GRU attention model give more prediction accuracy.

TABLE II: THE TIME RANGE OF DATA

Exchange	Start Date	End Date
Binance	2021-01-30	2021-12-23
Coinbase	2021-11-05	2021-12-24
Huobi	2020-11-03	2021-09-15
Kraken	2020-06-25	2021-09-15
KuCoin	2021-02-15	2021-12-24

Table 2 shows the start time and end time of data taken for each crypto exchange. The hyperparameters, such as learning rate, batch size, and the number of hidden layers and neurons significantly improve the model's performance. Sensitivity analysis can vary these parameters, to determine their impact on the model's accuracy and ability to detect anomalies. The real trading volume is plotted as a continuous line. The predicted trading volume is plotted as a continuous line. The upper and lower bounds are represented with dashed lines. Detected anomalies are marked as red dots. The x axis is labelled as the date, the y axis is labelled as trading volume in US dollars (USD). The custom attention layer focusses on the most relevant time steps of the input sequence. When the method (LSTM_attention, GRU_attention, RNN_attention) is specified, the model with the custom attention layer is created and trained. The lower bound is calculated as $3 \cdot \text{std}(\text{testy}) - \text{predicted values}$, where

testy is the actual values and predicted values are the values predicted by the model. The upper bound is $3 * \text{std}(\text{testy}) + \text{predicted values}$ and std is the standard deviation. Thus the actual values(blue), predicted values (orange), upper bound, lower bound and anomalies are shown in Figure 1

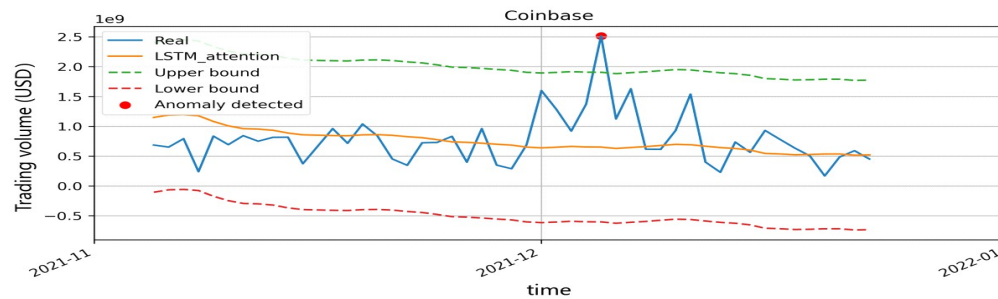


Fig. 1. Abnormal Transaction Detection for Coinbase

Key points regarding abnormal transaction detection for Coinbase include, identification of key factors, detection of anomalies, market integrity and methodological framework. Here orange line represents the transactions that are above normal, in the context of transaction volume but cannot be classified as abnormal transactions.

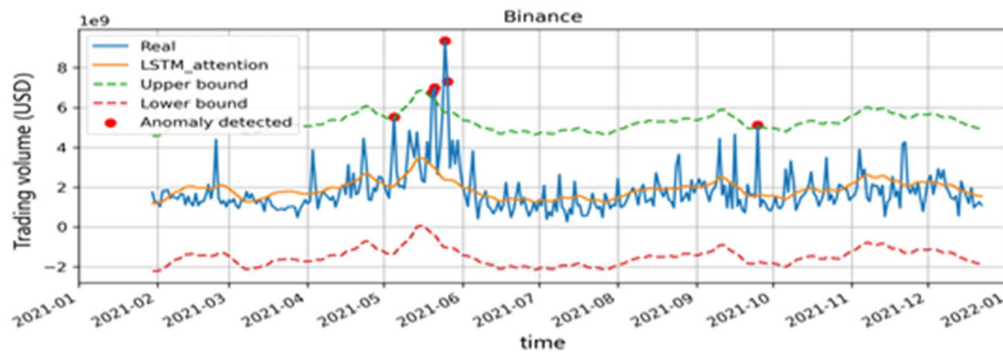


Fig. 2. Abnormal Transaction Detection for Binance.

The green line represents normal transactions that fall within the baseline or expected range of transaction amounts. The red points in the spike of the real data that touch the upper bound are the anomalous transactions shown in Figure 2 for the Binance crypto exchange. The data is split in to smaller sequences, using a sliding window approach. Here `datasplit(seq_length)` function splits the data into small windows for both testing and splitting. In testing phase the function uses the sliding window to predict future values for evaluation. Here prediction length and sequence length can be set, where prediction length is the time steps ahead one wants to predict and sequence length is the window size for the input data.

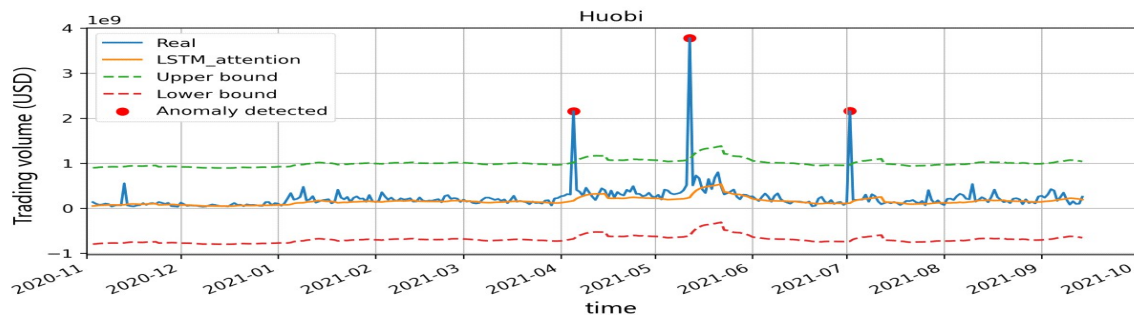


Fig. 3. Abnormal Transaction Detection for Huobi.

The model can flag significant deviations as potential anomalies by comparing the predicted transaction amounts with the actual amounts. The predicted transaction amounts are shown in orange.

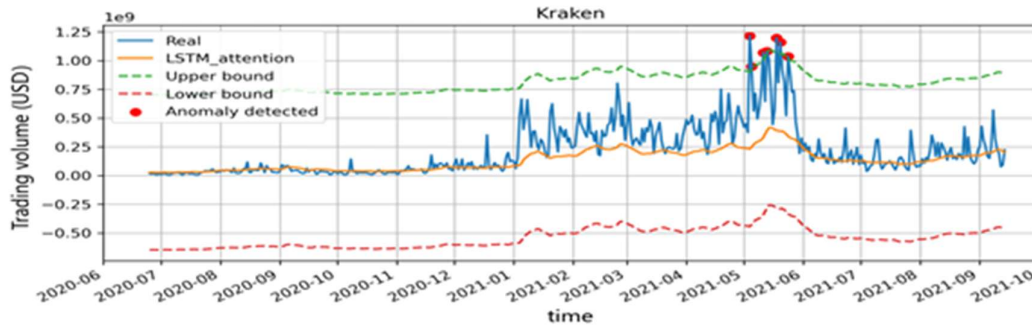


Fig .4. Abnormal Transaction Detection for Kraken

The red spike detected is the anomalous transaction shown in Figure 4 for Kraken crypto exchange.

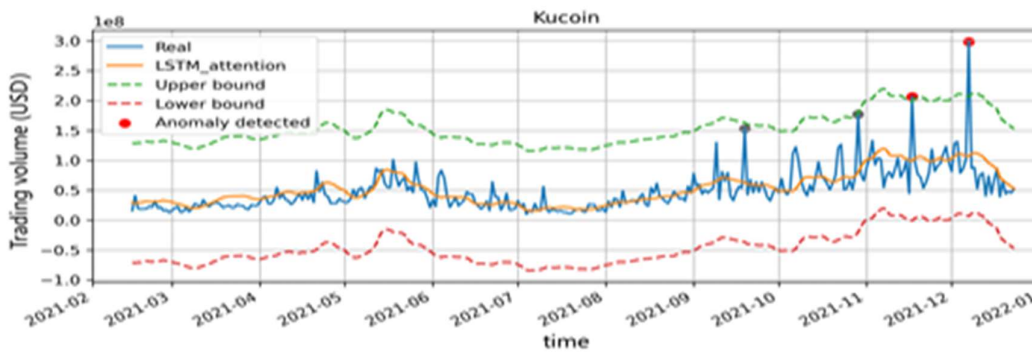


Figure 5. Abnormal Transaction Detection for Kucoin.

The red spike detected is the anomalous transaction shown in Figure 5 for the Kucoin crypto exchange. The results of the GRU with attention model is shown below in Figure 6.

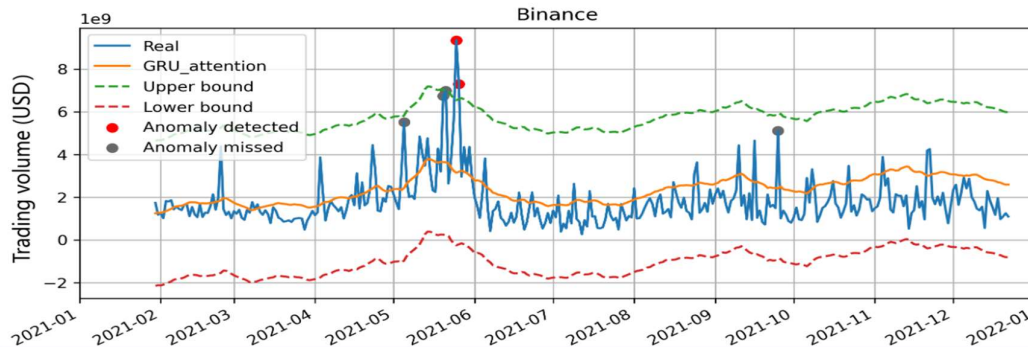


Figure 6 Detecting anomaly in Binance

This plotting and anomaly detection section visually represents how well the model's predictions align with real data, helping in identifying when abnormal events occur. A custom attention layer is implemented to enhance focus on important features in the input data sequence. The attention layer defines a trainable weight matrix W and a bias vector b , initialized to focus on specific features. These are used to compute attention scores for each time step in the sequence. The scores are calculated using a sigmoid activation applied to the weighted input sequence, enhanced by the bias term. This step ensures the model evaluates the importance of each feature in the sequence. A softmax function is applied to the scores to convert them into probabilities (a_t) representing each feature's importance relative to others. The attention weights scale the input sequence, and a weighted sum is computed, highlighting the most relevant features while suppressing irrelevant ones. The GRU model is used with `return_sequences=True`, ensuring that the output retains the temporal dimension necessary for attention.

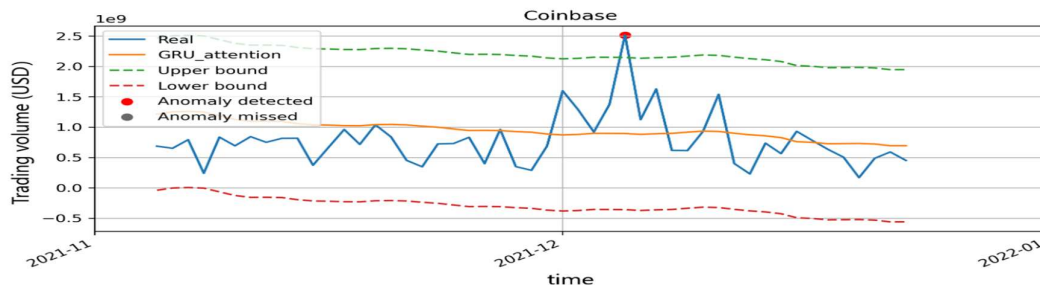


Figure 7 Detecting anomaly in Coinbase

Figure 6, the anomaly detection in Binance is shown, with the metrics that are considered are transaction volume, number of transactions, active users, price fluctuations, historical transaction patterns, market sentiment indicators, and regulatory events. Figure 7 shows the detection of an anomaly in the coinbase crypto exchange which takes into consideration metrics such as the transaction volume, number of transactions, unique active users, account balances, inbound and outbound transfers, market price changes and historical data patterns.

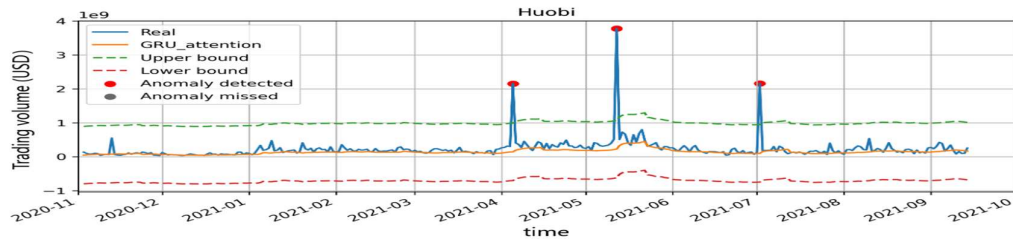


Figure 8 Detecting anomaly in Huobi

Figure 8 shows the anomaly detection in the Huobi crypto exchange. Transaction fees are yet another metric that is taken in to account for considering anomalies in the Huobi crypto exchange apart from the other metrics considered in the other exchanges.

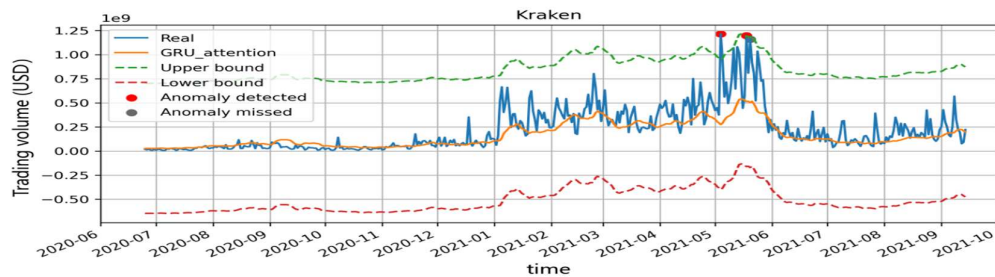


Figure 9 Detecting anomaly in Kraken.

Figures 9 and 10 show the detection of anomalous transactions in Kraken and in Kucoin. Both Kraken and Kucoin share similar metrics that are relevant for detecting anomalies in transaction amounts, including transaction volume, user activity metrics, account balances, inbound and outbound transfers, market price changes, historical data patterns, and correlation coefficients.

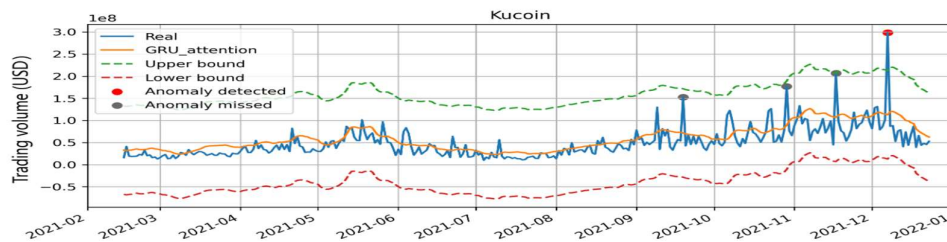


Figure 10 Detecting anomaly in Kucoin.

The model's performance depends on RMSE (Root Mean Square Error), MAE (Mean Absolute Error), and MAPE (Mean Absolute Percentage Error). This analysis helps identify the best parameter values for the model by showing how each parameter adjustment affects error levels across different exchanges.

TABLE III: METRICS OF TIME SERIES DEEP LEARNING MODELS

Exchange	LSTM RMSE	LSTM MAE	LSTM MAPE	LSTM _Attention RMSE	LSTM _Attention MAE	LSTM _Attention MAPE	GRU RMSE	GRU MAE	GRU MAPE
Binance	0.12	0.09	0.63	0.10	0.07	0.45	0.10	0.06	0.40
Coinbase	0.13	0.09	0.42	0.13	0.09	0.53	0.12	0.09	0.58
Huobi	0.07	0.02	0.34	0.07	0.02	0.32	0.07	0.02	0.34
Kraken	0.27	0.18	0.95	0.14	0.08	0.53	0.11	0.06	0.50
Kucoin	0.08	0.05	0.27	0.08	0.05	0.35	0.77	0.04	0.31

VI. CONCLUSION AND FUTURE WORK

The project introduces a novel framework for anomaly detection in cryptocurrency exchange trading volumes. This framework employs on-chain data gathering, and correlation analysis to pinpoint key influencing factors, and leverages an LSTM_attention deep learning model for predictive analysis. By amalgamating transaction data from leading exchanges and utilizing correlation insights, the system accurately forecasts transaction amounts.

REFERENCES

- [1] Chainalysis, Report: Key players of the cryptocurrency ecosystem who's who on the blockchains? 2021, <https://go.chainalysis.com/key-players-in-crypto-report.html>.
- [2] W. Chen, J. Wu, Z. Zheng, C. Chen, Y. Zhou, Market manipulation of bitcoin: Evidence from mining the Mt. Gox transaction network, in: 2019
- [3] IEEE Conference on Computer Communications, IEEE, 2019, pp. 964–972.
- [4] Bloomberg, South african brothers vanish, and so does \$3.6 billion in bitcoin, 2021, <https://www.bloomberg.com/news/articles/2021-06-23/s-african-brothers-vanish-and-so-does-3-6-billion-in-bitcoin>.
- [5] T. Li, D. Shin, B. Wang, Cryptocurrency pump-and-dump schemes, 2021, Available at SSRN 3267041.
- [6] C.C. Aggarwal, An introduction to outlier analysis, in: Outlier Analysis, Springer International Publishing, Cham, 2017, pp. 1–34, http://dx.doi.org/10.1007/978-3-319-47578-3_1.
- [7] R. Chalapathy, S. Chawla, Deep learning for anomaly detection: A survey, 2019, arXiv preprint arXiv:1901.03407.
- [8] Y. LeCun, Y. Bengio, G. Hinton, Deep learning, Nature 521 (7553) (2015) 436–444.
- [9] D.C. Montgomery, E.A. Peck, G.G. Vining, Introduction to Linear Regression Analysis, John Wiley & Sons, 2021.
- [10] D.W. Hosmer Jr., S. Lemeshow, R.X. Sturdivant, Applied Logistic Regression, vol. 398, John Wiley & Sons, 2013.
- [11] Y.-Y. Song, L. Ying, Decision tree methods: Applications for classification and prediction, Shanghai Arch. Psychiatry 27 (2) (2015) 130.
- [12] I. Rish, et al., An empirical study of the naive Bayes classifier, in: IJCAI 2001 Workshop on Empirical Methods in Artificial Intelligence, 3, (22) 2001, pp. 41–46.
- [13] A. Liaw, M. Wiener, et al., Classification and regression by randomforest, R News 2 (3) (2002) 18–22.
- [14] J.T. Connor, R.D. Martin, L.E. Atlas, Recurrent neural networks and robust time series prediction, IEEE Trans. Neural Netw. 5 (2) (1994) 240–254.
- [15] F.A. Gers, J. Schmidhuber, F. Cummins, Learning to forget: Continual prediction with LSTM, Neural Comput. 12 (10) (2000) 2451–2471.