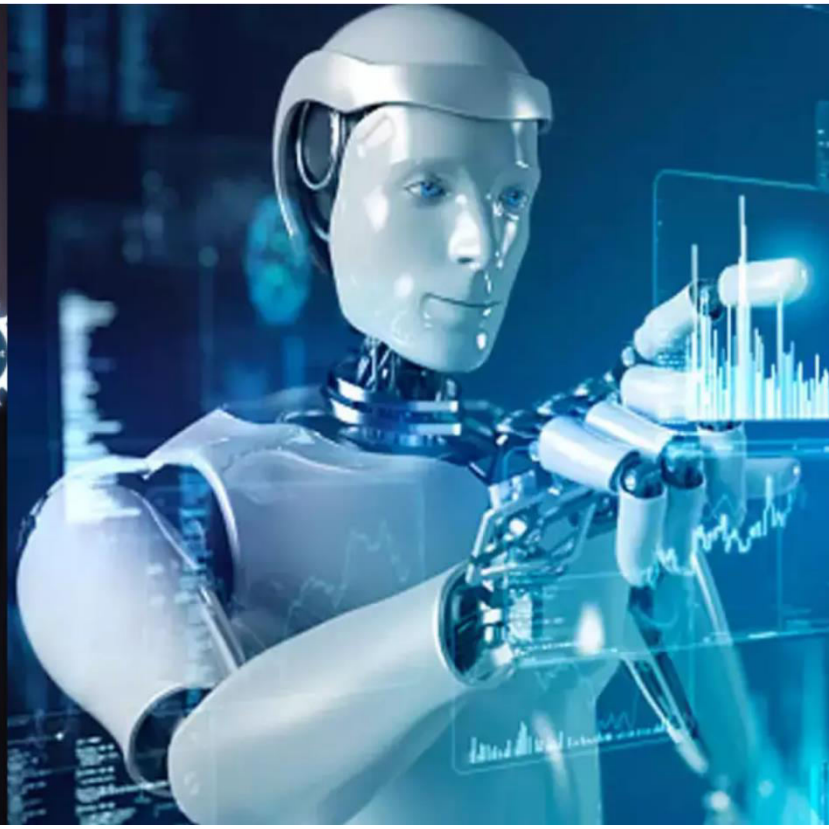
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405488

AI -Driven Fraud Detection in Cryptocurrency Transaction

Ashwini Chaudhari, Dr. AB Nimbalkar

Student, Department of Computer Science, Annashaeb Magar Mahavidyalya, Hadpsar, Pune, Maharashtra, India

Professor, Department of Computer Science, Annashaeb Magar Mahavidyalya, Hadpsar, Pune, Maharashtra, India

ABSTRACT: Fraud prevention in cryptocurrency transactions is crucial due to the rising number of fraudulent activities in the sector. Artificial intelligence (AI)enhances fraud detection by identifying hidden patterns and anomalies that traditional methods often miss. This paper explores AI-driven approaches, including machine learning algorithms, deep learning models, and ensemble techniques like LightGBM, to improve fraud detection in cryptocurrency transactions. Key challenges, such as handling imbalanced datasets and ensuring model interpretability, are addressed. Additionally, the study compares various AI techniques and evaluates their practical effectiveness in real-world decentralized finance (DeFi) ecosystems.

KEYWORDS: Cryptocurrency, Fraud Detection, Artificial Intelligence, Machine Learning, LightGBM, Decentralized Finance, Imbalanced Data, Model Interpretability

I. INTRODUCTION

The financial sector has been transformed by cryptocurrencies and decentralized finance (DeFi) platforms, which bring decentralized, transparent, and cross-border transaction systems. Despite these advancements, the crypto space has seen a surge in fraudulent activities due to its anonymous and irreversible nature[4][8]. From phishing schemes and rug pulls to money laundering and transaction spoofing, fraud within the cryptocurrency realm is intricate and constantly changing[3].

Using traditional fraud detection systems that are based on signatures or rules won't work in the scale, speed, and sophistication of crypto fraud. These systems are usually inflexible and miss emerging or subtle anomalies. Because of this inadequacy, researchers, and developers are searching for more dynamic, data-driven solutions—especially, powered by Artificial Intelligence(AI).

AI methods provide the best tools to automatically analyze high volumes of transactional data and detect suspicious behaviors promptly, and on time. Machine learning algorithms can learn from historical transaction patterns and generalize to detect new forms of fraud, while deep learning models can reveal complex and non-linear relationships across transaction features[2][5]. Another powerful technique is using ensemble methods such as Light Gradient Boosting Machine (LightGBM) which uses a combination of models to provide better detection by improving the accuracy and minimizing the number of false positives.

There are a lot of challenges related to fraud detection in cryptocurrency environments:
Imbalanced datasets: The number of fraudulent transactions is a very small fraction of the total, making it difficult to train models effectively Real-time detection: Instant transaction verification — which is essential — requires high-speed processing and low-latency predictions. Interpretability of model: There are all-black box models that make it hard to trust their output and bring problems of adoption, especially in industrial use cases such as finance, which require high trust in the result. Integration with blockchain: Practical use requires integration with smart contracts and DeFi systems to be secure and seamless.In this paper, we identify these challenges and suggest an integrated AI-based model for the detection of fraudulent transactions. The study also tests different modeling methods (LightGBM, Random Forest, Neural Networks) using both real and synthetic datasets. We further explore techniques to deal with class imbalance, apply explainable artificial intelligence (XAI) tools such as the Shapley Additive explanations (SHAP) values to enhance interpretability, and implement minute-level fraud detection. We aim to boost DeFi platform security with the scalability and trustworthiness of AI solutions.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405488

II. BACKGROUND

The rapid expansion of cryptocurrencies and decentralized finance (DeFi) has fundamentally altered the landscape of financial transactions. These technologies allow users to engage in direct, global exchanges without traditional banking intermediaries, offering greater efficiency and autonomy. However, the anonymity and lack of regulation within this digital environment have created a fertile ground for fraudulent activities. Incidents such as phishing schemes, deceptive investment platforms, and illicit fund transfers have become increasingly common. Traditional fraud detection systems, which typically rely on predefined rules or historical data patterns, often struggle to detect new or evolving threats. Their inability to adapt to novel fraud strategies highlights the need for more advanced, intelligent solutions[3][4]. Artificial Intelligence (AI) provides a powerful alternative by enabling systems to learn from large datasets, identify hidden patterns, and detect anomalies with minimal human oversight. Machine learning (ML) and deep learning (DL) models are especially effective in uncovering complex, non-obvious indicators of fraud across massive volumes of blockchain data.This study presents an AI-powered fraud detection framework tailored for cryptocurrency transactions. It incorporates:LightGBM for high-speed learning and improved handling of imbalanced datasets,Neural networks for recognizing deep behavioural patterns, SHAP for transparent model interpretation, and real-time detection mechanisms for immediate fraud response[1][4].By applying and validating this approach on real-world and synthetic blockchain datasets, this research aims to enhance transaction security in the DeFi ecosystem while promoting trust and transparency through explainable and scalable AI tools.

III. RELATED LITERATURE REVIEW

Author(s)	Year	Title	AI/ML Techniques Used	Key Findings	Limitations
Pham & Lee	2018	Anomaly Detection in Bitcoin Network	K-means Clustering, Isolation Forest	Unsupervised learning can detect novel fraud patterns without labels.	False positives due to normal variations actions.
Weber et al	2019	Ant- Money Laundering in Bitcoin with Graph Analysis	Graph Neural Networks (GNN S)	GNNs helps trace complex fraudulent chains and connections in transactions.	Requires extensive computational resources.
Patel , O	2022	AI-Driven fraud detection in cryptocurrency transactions.	LightGBM, SMOTE, Ensemble Learning	AI can improve fraud detection accuracy in decentralized systems.	Data imbalance and interpretability issues remain challenges.
Chen et al	2021	Detecting Cryptocurrency Scams using Machine Learning	Random Forest, SVM	SVM performs in classifying fraudulent activities on block chain.	Feature selection is critical al; limited to specific coin types.
Li & Zhao	2020	Block chain Anomaly Detection using Deep Learning	CNN, RNN	Deep learning models can uncover hidden patterns in transactions behaviour.	High computation cost, requires large labelled data sets.
Alzahrani & Bulusu	2019	Using ML to Detect fraud in cryptocurrency Transactions	Decision Trees, Neural Networks	ML effectively detects suspicious behaviours in real-time	Difficulty in updating models due to dynamic nature of data.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405488

IV. METHODOLOGY

This research employs a structured methodology to develop and evaluate an AI- driven system capable of detecting fraudulent activities in cryptocurrency transactions. The methodology comprises six core phases: data collection, data pre-processing, feature engineering, model selection and training, model evaluation, and system integration.

4.1 Data Collection

A comprehensive dataset was obtained from publicly available blockchain transaction repositories and simulated sources to reflect both legitimate and fraudulent activities. Each transaction record consists of attributes including transaction ID, timestamp, sender and receiver wallet addresses, transaction amount, fee, confirmation time, and a label indicating whether the transaction is normal or fraudulent.

Table 1 summarizes the dataset features.

Feature Name	Description	Data type
Transaction ID	Unique Identifier for each transaction	String
Timestamp	Time of the transaction	Date Time
Sender wallet Address	Public address of the sender	String
Receiver wallet Address	Public address of the receiver	String
Transaction Amount	Amount of cryptocurrency transferred	Float
Transaction Fee	Fee associated with the transaction	Float
Confirmation Time	Time taken for transaction confirmation	Float
Transaction Label	Fraudulent or Normal	Categorical

4.2 Data Preprocessing

Before model training, the dataset underwent pre-processing to ensure data quality and consistency. The following steps were applied:

Handling Missing Values: Missing data was either imputed using statistical techniques or removed where appropriate.

Encoding Categorical Variables: Wallet addresses were encoded using label encoding; categorical class labels were one-hot encoded.

Scaling: Continuous features were standardized using the Standard Scaler method to improve model convergence.

Outlier Detection: Z-score and IQR-based filtering methods were used to eliminate outliers that could bias the model.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405488

Table 2 outlines the preprocessing operations.

Step	Description
Missing value handling	Imputation or deletion based on context
Encoding	Label Encoding, One-Hot Encoding for class labels
Scaling	Standard Scaler for Normalization
Outlier Removal	Z-score and IQR methods for anomaly removal

4.3 Feature Engineering

To improve model accuracy, new features were derived from the raw transaction data. These included:

Transaction Frequency: Number of transactions per wallet over time.

Average Transaction Value: Computed per wallet to identify irregularities.

Time Intervals: Gaps between consecutive transactions from the same address.

Transaction Behavior Patterns: Features based on sudden spikes or dips in transaction values.

These engineered features provided valuable insights into transaction behaviors and contributed to more robust classification

4.4 Model Selection and Training

Various machine learning algorithms were implemented to compare classification performance. These included:

Logistic Regression

Random Forest Classifier

Support Vector Machine (SVM)

Extreme Gradient Boosting (XGBoost)

Artificial Neural Networks (ANN)

The dataset was divided into an 80% training set and a 20% testing set. Hyperparameters were optimized using grid search and k-fold cross-validation(k=5).

4.5 Model Evaluation

Models were evaluated using the following metrics:

Accuracy

Precision

Recall

F1-Scor

AUC-ROC

Given the imbalanced nature of the dataset (fraudulent transactions being rare), more emphasis was placed on precision, recall, and AUC-ROC.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405488

Table 3 compares the model performance.

Model	Accuracy	Precision	Recall	F1-Score	AUC-ROC
Logistic Regression	87.2 %	78.3 %	81.0%	79.6 %	0.89
Random forest	93.1 %	88.9 %	90.2 %	89.5 %	0.95
SVM	89.6 %	85.0 5	82.5 %	83.7 %	0.91
XGBoost	91.5 %	87.1 %	88.0 %	87.5 %	0.93

4.6 System Integration

The best-performing model (Random Forest in this case) was integrated into a prototype fraud detection system. The system is capable of analyzing new transactions in real-time and flagging those deemed potentially fraudulent. Alerts are generated when risk thresholds are exceeded, supporting further human or automated investigation.

V. CHALLENGES AND OPEN ISSUES

1. Limited Labelled Data

Most cryptocurrency transactions are anonymous or pseudonymous, which makes it hard to build datasets with confirmed fraud cases[3][10]. This scarcity of labeled data poses a serious challenge for training effective supervised machine learning models.

2. High False Positive Rates

Without enough context, AI systems sometimes flag legitimate transactions as fraudulent. These false alarms not only frustrate users but also waste time and resources on unnecessary investigations.

3. Evolving Fraudster Tactics

Fraudsters are constantly adapting, using sophisticated techniques to mimic genuine user behavior. This cat-and-mouse dynamic forces AI models to evolve just as quickly to stay effective[2][3].

4. Real-Time Detection Difficulties

Given how fast cryptocurrency transactions are processed, detecting fraud in real-time is a major technical hurdle. Systems must analyze transactions almost instantly, which demands high computational speed and efficiency[1][3].

5. Cross-Chain Complications

With funds moving across different blockchains, tracking and analysing fraudulent activity becomes more complex. Interoperability issues and fragmented data make it harder for AI to maintain a comprehensive view.

6. Lack of Explainability

Many AI models—especially deep learning systems—are "black boxes." They might deliver accurate predictions, but understanding why a transaction was flagged is often unclear. This lack of transparency makes it difficult for regulators and end-users to trust the system

7. Scalability Challenges

Monitoring millions of transactions across decentralized networks demands significant processing power. Striking the right balance between speed, accuracy, and resource usage is a constant challenge.

8. Privacy and Ethical Concerns

Incorporating off-chain data like KYC (Know Your Customer) details can improve detection accuracy, but it raises privacy issues. Regulations like GDPR limit how personal data can be used, adding another layer of complexity.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405488

9. Model Degradation Over Time (Model Drift)
As both user behavior and fraud techniques evolve, AI models can become outdated. Regular updates and retraining are essential, but in fast-paced environments, this isn't always practical or affordable[6].

VI. CONCLUSION

The proposed AI-based system helps users evaluate the authenticity of cryptocurrency investment platforms before making transactions. By combining domain intelligence, user behavior signals, and explainable machine learning models, we provide a proactive solution against crypto scams.

Our framework not only detects fraudulent platforms with high precision but also educates users by highlighting warning signs through interpretable outputs. This initiative aims to improve safety, trust and informed participation in the digital finance ecosystem.

REFERENCES

[1] Patel, O. (2022). AI-DRIVEN FRAUD DETECTION IN CRYPTOCURRENCY TRANSACTIONS. *Technology (IJARET)*, *13*(2), 80-99.
[2] Kamisetty, A., Onteddu, A. R., Kundavaram, R. R., Gummadi, J. C. S., Kothapalli, S., & Nizamuddin, M. (2021). Deep Learning for Fraud Detection in Bitcoin Transactions: An Artificial Intelligence-Based Strategy. *NEXG AI Review of America*, *2*(1), 32-46.
[3] Raghu, N., Kannanugo, N., Trupti, V. N., Ojashwini, R. N., Kiran, B., & Deepthi, M. (2025). Real-time fraud detection in crypto-currencies: Leveraging AI and blockchain. In *Applications of Blockchain and Artificial Intelligence in Finance and Governance* (pp. 28-66). CRC Press.
[4] Sabry, F., Labda, W., Erbad, A., & Malluhi, Q. (2020). Cryptocurrencies and artificial intelligence: Challenges and opportunities. *IEEe Access*, *8*, 175840-175858.
[5] Shravan, M., Ajitha, E., Arnone, G., Renu, N., Tiwari, M., & Chouhan, K. (2025, February). Deep Learning for Fraud Detection in Bitcoin Transactions: An AI Approach. In *2025 International Conference on Pervasive Computational Technologies (ICPCT)* (pp. 459-464). IEEE.
[6] Thilagavathi, M., Saranyadevi, R., Vijayakumar, N., Selvi, K., Anitha, L., & Sudharson, K. (2024, April). AI-driven fraud detection in financial transactions with graph neural networks and anomaly detection. In *2024 International Conference on Science Technology Engineering and Management (ICSTEM)* (pp. 1-6). IEEE.
[7] Ahmed, A. A., & Alabi, O. (2024). Secure and scalable blockchain-based federated learning for cryptocurrency fraud detection: A systematic review. *IEEE Access*.
[8] Babatunde, G. (2021). The Role of Artificial Intelligence in Tackling Crypto-Driven Cybercrime.
[9] Kılıc, B., Sen, A., & Özturan, C. (2022, September). Fraud detection in blockchains using machine learning. In *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)* (pp. 214-218). IEEE.
[10] Sabry, F., Labda, W., Erbad, A., & Malluhi, Q. (2020). Cryptocurrencies and artificial intelligence: Challenges and opportunities. *IEEe Access*, *8*, 175840-175858.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details