© May 2026 | IJIRT | Volume 12 Issue 12 | ISSN: 2349-6002

ChainGuard: AI-Powered Money Laundering Detection over Blockchain Networks

Prof R. N. Devray[1], Sneha Sharad Bhapkar[2], Renuka Santosh Kardile[3],
Rutuja Narayan Mote[4], Vaishnavi Dnyandev Wani[5]
[1]*Department of Computer Engineering, Dr. Vithalrao Vikhe Patil College of Engineering, Ahilyanagar, India*
[2,3,4,5]*Student, Department of Computer Engineering Dr. Vithalrao Vikhe Patil College of Engineering Ahilyanagar, India*

***Abstract*—Money laundering has become increasingly complex with the rise of digital payment systems and blockchain-based financial platforms. Traditional Anti-Money Laundering (AML) frameworks rely mainly on static rules and manual investigation, which often fail to identify evolving fraudulent behaviors and generate high false-positive rates. To address these limitations, this research proposes BlockDetect, an intelligent AML detection framework that integrates machine learning techniques with blockchain transaction analytics. The system extracts behavioral and structural features from blockchain data, analyzes wallet interactions, and classifies transactions based on their likelihood of being suspicious. Machine learning algorithms, such as Random Forest and XGBoost, are employed to detect anomalous patterns commonly associated with layering, structuring, and circular money flows. The approach enhances accuracy, reduces manual effort, and provides an interpretable decision-support mechanism for AML investigators. The study demonstrates that combining ML-based anomaly detection with blockchain transparency can significantly strengthen financial security and support early identification of illicit activities. The proposed framework serves as a scalable and adaptable solution for modern AML challenges in decentralized financial environments.**

***Index Terms*—BlockDetect, Anti-Money Laundering, Machine Learning, Blockchain, Data Classification, Python, Fraud Detection, etc.**

I. INTRODUCTION

The rapid digital transformation of financial systems and the widespread adoption of decentralized transaction platforms have increased the complexity of monitoring and detecting illicit monetary activities. Modern banking environments generate massive volumes of high-speed transactional data, making manual inspection and traditional rule-based Anti–Money Laundering (AML) techniques increasingly inadequate. Criminal actors now exploit digital wallets, online banking infrastructure, and cryptocurrency networks to conceal illegal funds through high-frequency transfers and multilayered trans-actions. These evolving laundering strategies underscore the need for intelligent, automated detection systems capable of analyzing diverse transaction attributes and identifying hidden irregularities in real time. [1]

Machine Learning (ML) has emerged as a highly effective approach for AML applications because of its ability to learn behavioral patterns from historical financial data and generalize them to new, unseen transactions. ML-driven classification, clustering, and anomaly detection methods enable the discovery of suspicious activities that remain undetected by static heuristic-based rules. However, the reliability and trustworthiness of ML-powered AML systems depend heavily on the accuracy and integrity of the underlying transaction data, as manipulated or incomplete records can compromise detection outcomes. [2]

Blockchain technology complements ML by offering transparency, immutability, and tamper-resistant data storage. Integrating blockchain mechanisms with ML-based transaction analysis enhances evidence traceability, supports secure audit trails, and improves confidence in AML decisions. This com-bination strengthens regulatory compliance, reduces the possibility of data manipulation, and supports real-time monitoring of suspicious financial behavior.

In this context, the proposed BlockDetect framework integrates machine learning techniques with blockchain-inspired security principles to identify and classify suspicious transactional patterns. The system analyzes user behavior, performs risk scoring, and securely stores detection outcomes to en-hance trust, auditability, and transparency in AML processes.

BlockDetect provides a unified platform that addresses the limitations of existing AML detection systems by combining advanced analytics with secure data handling. [2]

The primary contributions of this work are as follows:

1. Development of an ML-based framework for classifying suspicious and legitimate transactions;
2. Incorporation of blockchain-based verification concepts to enhance transparency and integrity;
3. Design of a modular architecture supporting feature extraction, risk analysis, and secure storage; and
4. Implementation of a user-friendly interface demonstrating real-world applicability of the model.[7]

II. LITERATURE SURVEY

Several researchers have investigated the integration of ma-chine learning and blockchain analytics for detecting money-laundering activities. Their studies highlight the importance of advanced data-driven techniques, graph analysis, and intelligent automation for identifying suspicious behaviors across cryptocurrency ecosystems.

- Examined how supervised machine-learning models can analyze blockchain transaction data to identify unusual or suspicious financial activities. Their findings show that combining classical features with blockchain-specific behavioral patterns significantly enhances AML detection accuracy. [1]
- Expanded on their earlier study by evaluating larger blockchain datasets. They emphasized the importance of address clustering, data preprocessing, and handling class imbalance to improve the reliability of machine-learning models in AML detection. [2]
- Introduced a subgraph contrastive learning approach for Bitcoin transactions. Their method learns structural differences between legal and illicit transaction subgraphs, enabling the detection of coordinated laundering activities that traditional supervised models may miss. [2]
- Proposed techniques to identify suspicious transaction subgraphs within blockchain networks. Their framework extracts potential laundering clusters using heuristics and then ranks them with machine-learning models, supporting analysts in detecting organized laundering rings. [3]
- Applied machine-learning algorithms to Ethereum ac-count behavior. They demonstrated that models such as Random Forest and neural networks can classify illicit accounts based on features like transaction frequency, gas usage, and interaction patterns. [4]
- Discussed the role of blockchain for secure financial applications. They highlighted blockchain's transparency, immutability, and auditability as strong foundations for detecting fraud and ensuring trusted transaction monitoring. [5]
- Reviewed machine-learning methods used for fraud and anomaly detection. They emphasized that the success of AML models depends heavily on dataset quality, proper feature selection, and continuous retraining to adapt to evolving laundering techniques. [6]
- Focused on mining transactional patterns using ML-based and statistical methods. Their study showed how temporal behavior, transfer patterns, and account interactions can help detect suspicious fund movements. [6]
- Investigated predictive models for cyber-fraud and financial misuse. They noted that combining multiple machine-learning techniques can increase precision and reduce false positives in financial anomaly detection. [7]
- Compared various classification algorithms for fraud prediction and found that ensemble models generally outperform individual classifiers when dealing with rare events such as money laundering. [8]

III. PROBLEM STATEMENT

The complexity of cryptocurrency transactions makes them a prime target for money laundering, while traditional ML systems fail to detect such activities effectively. Project aims to develop a machine learning-based system that can analyze blockchain transaction patterns and accurately classify wallets as suspicious or legal, ensuring scalable and reliable anti-money laundering detection.

IV. METHODOLOGY

The proposed work is designed to deliver an automated and secure framework capable of identifying potentially suspicious financial transactions. The methodology follows a structured multi-phase pipeline in which blockchain-based transactional records are analyzed using machine learning classifiers. The approach integrates the transparency and immutability of blockchain with the predictive intelligence of ML models, ensuring both reliable detection and trustworthy storage of results. The complete workflow is organized into five key stages: data acquisition, preprocessing, feature engineering, model development, and transaction categorization. This unified pipeline enables efficient fraud detection while preserving privacy and data integrity.

4.1 Overview of the Proposed System:

System is implemented as a web-driven intelligent monitoring platform built using Python and the Flask framework. At its core lies a trained machine learning model that evaluates large volumes of structured and semi-structured transaction data, classifying each record as legitimate or suspicious. The blockchain layer maintains an immutable audit trail by storing essential transaction and prediction outcomes, ensuring the results cannot be modified or deleted. A well-designed web interface supports analysts in examining alerts, visualizing behavioral trends, and generating compliance-oriented reports.

4.2 System Architecture Design:

The architecture comprises several coordinated layers re-sponsible for maintaining smooth data flow and accurate anomaly detection. Each component is described below:

a) Data Acquisition:

Blockchain transaction datasets are collected from publicly accessible block explorer APIs and re-search repositories. The dataset includes wallet identifiers, timestamps, transaction amounts, gas fees, and directional transfer patterns. When avail-able, labeled datasets containing confirmed illicit or fraudulent activity (e.g., scams, mixers, and phishing flows) are incorporated to support super-vised learning tasks.

b) Data Pre-processing Layer:

Raw blockchain data often contains inconsistencies, missing attributes, and noise. To ensure uniformity, the following preprocessing procedures are applied:

- Data Cleaning: Removal of corrupted entries, incomplete records, and abnormal values.
- Normalization: Scaling numerical fields such as transaction values and frequency using Min–Max normalization.
- Address Encoding: Transforming alphanumeric wallet IDs into numerical representations suitable for ML algorithms.
- Graph Construction: Building a transaction graph in which nodes represent wallet ad-dresses and edges represent fund transfers.

c) Model Training and Selection:

Multiple machine learning algorithms including Random Forest, XGBoost, Logistic Regression, and Decision Trees are trained to determine the most efficient model for detecting abnormal financial behavior. Training is performed on labeled datasets containing examples of both legitimate and suspicious transactions. Models are evaluated using standard metrics such as Accuracy, Precision, Recall, and F1-Score. Ensemble techniques such as Random Forest and XGBoost demonstrate superior performance due to their effectiveness in identifying nonlinear patterns and handling high-dimensional datasets.

d) Blockchain Integration Layer:

After classification, each prediction (legitimate or suspicious) is securely written to the blockchain to maintain transparency and tamper-proof logging. This layer ensures that no external entity can alter the stored detection outcomes, strengthening auditability and compliance.

e) Web Application Layer:

The trained ML model is deployed through a Flask-based web interface, enabling users to:

- Upload transaction datasets
- View prediction outcomes and associated risk categories
- Explore network visualizations and suspicious cluster formations
- Generate analytical reports to support AML

investigations

This interface supports real-time detection, making it easier for investigators to monitor and analyze transaction flows.

f) Database Layer:

A MySQL database stores user credentials, processed transaction logs, model results, and meta-data linked with blockchain hashes. This hybrid storage strategy combines the retrieval efficiency of traditional databases with the reliability and immutability of blockchain technology.

4.3 Workflow of the System:

The operational flow of BlockDetect is summarized below:

- Transaction data is uploaded by an administrator or fetched from live data feeds.
- The preprocessing unit cleans, filters, and normalizes the incoming data.
- The refined dataset is passed to the trained ML classification model.
- Each transaction is categorized as normal or suspicious.
- Suspicious transactions are recorded on the blockchain for verifiable tracking.
- The admin dashboard displays visual analytics, risk summaries, and potential red-flag patterns.

Overall, the proposed system integrates Machine Learning and Blockchain Technology to establish a secure, transparent, and intelligent AML detection mechanism, as illustrated in "Fig. 1".

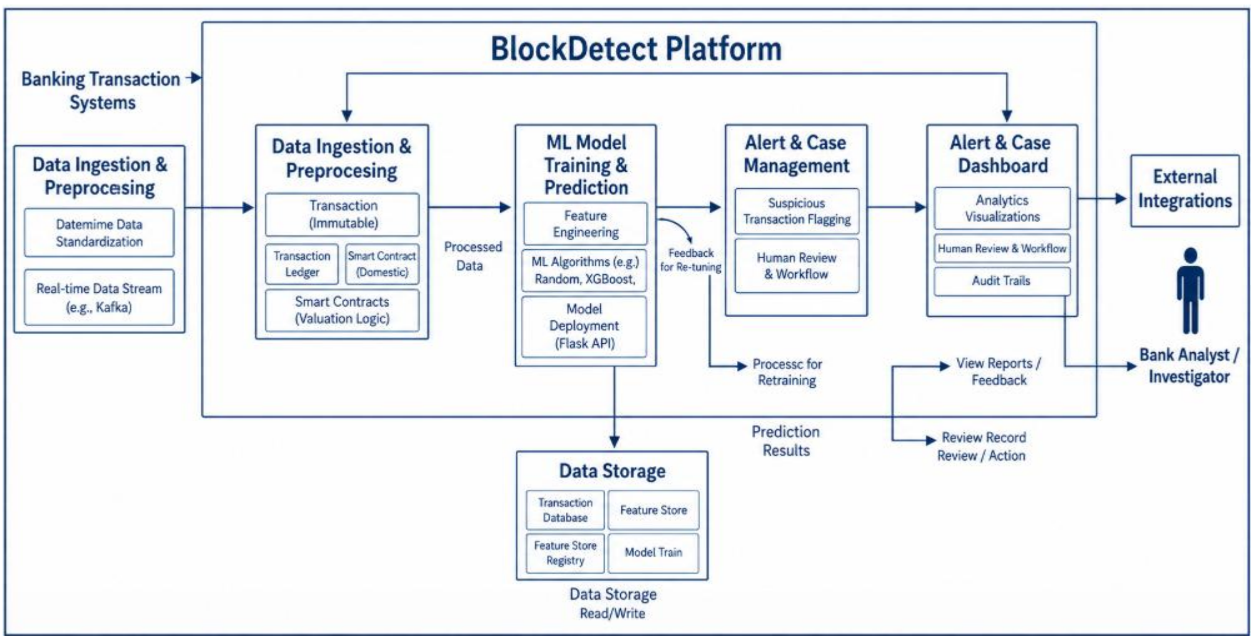

Fig. 1. Architecture Diagram

The BlockDetect system operates by gathering structured transaction data, securing it within a blockchain ledger, and analyzing it through machine learning techniques. The ML component identifies deviations from normal financial be-haviour, while the blockchain component guarantees secure, immutable storage of results. A Flask-based web dashboard enables administrators to upload data, monitor alerts, and ex-amine suspicious transaction flows in real time. By combining blockchain for data integrity and ML for intelligent prediction, the system provides a more robust and efficient approach for detecting money laundering activities.

V. RESULTS AND DISCUSSION

The proposed BlockDetect system was evaluated using real-time transaction data through a web-based dashboard interface. The system successfully classified transactions into legal and suspicious categories using trained machine learning models.

A. Dataset Summary

The system processed a total of 62 transactions, out of which:

- 25 transactions were classified as illegal
- 37 transactions were classified as legal
- The overall illegal transaction rate was 40.32%

This demonstrates the system's ability to effectively distinguish between normal and suspicious financial activities.

B. Classification Results Visualization

The distribution of legal and illegal transactions is illustrated in Fig. 2. Legal transactions account for 59.7%, while illegal transactions account for 40.3%. This visualization helps in understanding the proportion of fraudulent activities detected within the dataset.

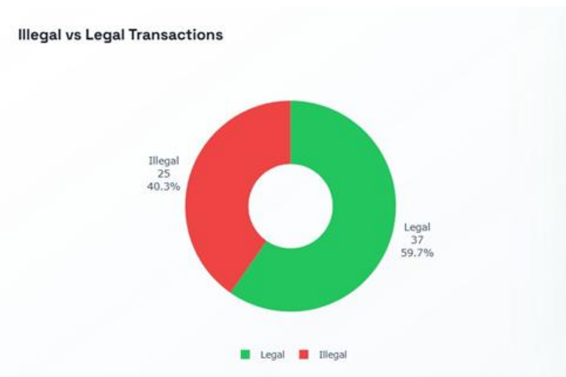

Fig. 2. Distribution of Legal and Illegal Transactions

C. Model Performance Evaluation

The performance of the machine learning model was eval-uated using key metrics such as Precision, Recall, F1-Score, and Accuracy. The results are summarized in Table I.

Table I: Performance Metrics of the Proposed Model

Metric	Value (%)
Precision	98.57
Recall	98.59
F1-Score	98.56
Accuracy	98.59

D. Performance Analysis

The results indicate that the proposed model achieves very high performance:

- Accuracy (98.59%) shows that the model correctly classifies most transactions.
- Precision (98.57%) indicates a low false positive rate.
- Recall (98.59%) confirms that most illegal transactions are successfully detected.
- F1-Score (98.56%) reflects a balanced performance between precision and recall.

E. Graphical Representation

The graphical comparison of model performance is shown in Fig. 3.

Fig. 3. Model Performance Metrics

VI. DISCUSSION

The experimental results confirm that the BlockDetect system performs efficiently in identifying suspicious transactions with high accuracy. The integration of Machine Learning with Blockchain ensures both accurate classification and secure, tamper-proof storage of transaction data.

Compared to traditional rule-based systems, the proposed approach significantly improves detection capability and re-duces manual effort. The system is scalable and suitable for real-world financial and cryptocurrency applications.

VII. CONCLUSION

The project BlockDetect: A Smart Anti-Money Laundering Detection System using Machine Learning aims to offer a clever and effective way to identify and stop money laundering activities in a variety of banking and financial transactions. Transparency, data security, and real time fraud detection are all improved by the system's integration of Machine Learning (ML) and Blockchain technology. Blockchain technology and machine learning algorithms work together to guarantee both the safe and impenetrable storage of transactional data as well as the precise categorization of questionable transactions. The gathering and preprocessing of financial statistics, creating an efficient system architecture, and putting strong categorization models into practice were all major priorities during the project's development. An interactive and user-friendly web-based interface where authorized users can examine transaction data, see trends, and keep an eye on high-risk activity was made possible by the use of Python and the Flask framework. By examining important transaction characteristics and past records, the system effectively detects fraudulent behavior patterns, offering high accuracy and quicker decision-making assistance.

VIII. FUTURE WORK

Future enhancements of the BlockDetect system may focus on integrating more advanced deep learning architectures to further improve detection accuracy and adaptability. Incorporating real-time streaming data from live banking networks could enable continuous monitoring of financial transactions without manual uploads. Additional features such as cross-border transaction tracking, multi-bank connectivity, and mobile application access may significantly expand the system's usability.

To support a larger user base and high transaction through-put, the blockchain framework can be scaled by adopting distributed consensus mechanisms or hybrid storage solutions. With these enhancements, BlockDetect has the potential to evolve into a comprehensive, industry-grade tool for combating financial crimes and strengthening global anti-money laundering efforts.

ACKNOWLEDGMENT

We sincerely express our gratitude to the researchers and publishers for making their valuable resources accessible. We are also deeply thankful to our guide and reviewers for their constructive suggestions, and we extend our appreciation to the college authorities for providing the necessary infrastructure and support.

REFERENCES

[1] A. Venčkauskas, Š. Grigaliūnas, L. Pocius, R. Brūzgienė, and A. Romanovs, "Machine learning in money laundering detection over blockchain technology," IEEE Access, vol. 13, pp. 7555–7573, 2025, doi: 10.1109/ACCESS.2024.3452003.

[2] S. Ouyang, Q. Bai, H. Feng, and B. Hu, "Bitcoin money laundering detection via subgraph contrastive learning," Entropy, vol. 26, no. 3, Art. no. 211, 2024, doi: 10.3390/e26030211.

[3] K. Song, M. A. Dhraief, M. Xu, L. Cai, X. Chen, A. Arvind, and J. Chen, "Identifying money laundering subgraphs on the blockchain," in Proc. 5th ACM Int. Conf. AI in Finance (ICAIF), 2024, doi: 10.1145/3677052.3698635.

[4] C. Obi-Okoli, O. Jogunola, B. Adebisi, and M. Hammoudeh, "Machine learning algorithms to detect illicit accounts on Ethereum," in Proc. Int. Conf. Future Networks and Distributed Systems (ICFNDS), 2023, pp. 747–752, doi: 10.1145/3644713.3644838.

[5] Q. Wang, W.-T. Tsai, and B. Du, "RMGANets: Reinforcement learning-enhanced multi-relational attention graph-aware network for anti-money laundering detection," Complex & Intelligent Systems, 2024, doi: 10.1007/s40747-024-01615-9.

[6] S. Farrugia, J. Ellul, and G. Azzopardi, "Detection of illicit accounts over the Ethereum blockchain," Expert Systems with Applications, vol. 150, Art. no. 113318, 2020, doi: 10.1016/j.eswa.2020.113318.

[7] J. R. Oliveira et al., "Enhancing anti-money laundering protocols: Employing machine learning to minimise false positives and improve operational cost efficiency," in Proc. ACM Conf., 2024, doi: 10.1145/3704137.3704156.

[8] A. Bella Baci, K. Brousmiche, I. Amal, and F. Abdelhédi, "Detecting illicit Ethereum accounts based on their transaction history and properties using machine learning," in Proc. Int. Conf. Deep Learning, Big Data and Blockchain (DBB), 2022, pp. 97–108, doi: 10.1007/978-3-031-16035-6_8.

[9] H. X. et al., "Effective illicit account detection on large cryptocurrency graphs (DIAM)," in Proc. ACM Conf., 2024, doi: 10.1145/3627673.3679707.

[10] H. Nasir Mohammed, N. S. Malami, and S. Thomas, "Machine learning approach to anti-money laundering: A review," in Proc. IEEE Nigeria 4th Int. Conf. Disruptive Technologies

for Sustainable Development (NIGERCON), 2022, doi: 10.1109/NIGERCON54645.2022.9803072.

[11] J. Gayta, "Is it possible to hack cryptocurrency?" Accessed: Nov. 1, 2023. [Online]. Available: https://www.congatec.com/en/research/publications/crypto-hacks-exploits-by-method

[12] J. Golosova and A. Romanovs, "The advantages and disadvantages of the blockchain technology," in Proc. IEEE 6th Workshop Advanced Information, Electronic and Electrical Engineering, Nov. 2018, pp. 1–6.

[13] E. B. Stransky, A. Chess, E. Gamadani, M. Green, I. Maers, F. Tönnies, and M. Virza, "Research: Decentralized anonymous payments from Bitcoin," in Proc. IEEE Symp. Security and Privacy, May 2014, pp. 459–474.

[14] Y. A. Li, Q. W. Su, S. Y. Wu, M. H. Au, and D. Liu, "Tracing the Monero blockchain transactions: Crypto examiner with an enhanced transaction model," IEEE Trans. Dependable and Secure Computing, vol. 21, pp. 679–691, Mar. 2024.

[15] S. Foley, J. Karlsen, and T. J. Putnis, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?" Review of Financial Studies, vol. 32, no. 12, pp. 3889–3923, 2019.

[16] M. Lin, H. Chen, and J. Yan, "Detecting cycles of money laundering in Bitcoin mixing transactions," Algorithmica, vol. 78, pp. 1063–1090, 2020.

[17] A. Mooney, "Cryptocurrency laundering," in Regulating the Metaverse Economy: Resources, Practices, Advancements. Springer, 2023, pp. 287–322.

[18] A. Shaghaghi, A. Dehghantanha, and K. R. Choo, "Challenges in blockchain forensics," Digital Investigation, vol. 26, pp. S47–S55, 2021.

[19] M. N. R. Zotos, S. Chaurasia, and D. Shukla, "Mixers detection in Bitcoin network: A step towards detecting money laundering in cryptocurrencies," in Proc. IEEE Int. Conf. Big Data, Dec. 2022, pp. 5775–5782.

[20] A. Shirogliannis, A. P. Mountrouidou, and B. Bahri, "Mixing detection on Bitcoin transactions using statistical patterns," IEEE Blockchain, vol. 3, pp. 136–148, Sep. 2023.