GOVERNMENT FUND ALLOCATION AND TRACKING SYSTEM USING BLOCKCHAIN TECHNOLOGY

K.M. Ravi Kumar[1], Tanuj Jenna[2], P. Abhishek[3], B. Lakshman[4], S. Kavya[5]

[1]Department of Computer Science and Engineering (AI & ML)

Avanthi Institute of Engineering & Technology (Autonomous), Vizianagaram, India

Kmravikumar9@gmail.com[1], tanujjenna2004@gmail.com[2], abhishekputta62@gmail.com[3], ramulaxman959@gmail.com[4], sasapukavya5@gmail.com[5]

Abstract

For regulatory bodies around the world, financial crime via cryptocurrency channels poses growing challenges. The pseudonymous nature and quick transaction speeds of blockchain networks pose a challenge to conventional 3 anti-money laundering systems. In order to detect illegal financial activity in real time, this study presents an integrated framework that combines sophisticated machine learning algorithms with immutable blockchain ledger technology. The suggested system employs XGBoost-based analytics and Artificial Neural Networks to identify intricate money laundering patterns that are challenging to identify with conventional rule-based techniques. The proposed system uses Artificial Neural Networks and XGBoost-based analytics to detect complex money laundering patterns that are difficult to detect using 149 conventional rule-based methods. The architecture uses smart contracts to achieve transaction immutability while maintaining computational efficiency. It is implemented on Ethereum using Ganache simulation. Experimental validation demonstrates detection accuracy exceeding 92% in simulated laundering scenarios with an alert generation latency of less than two seconds. The system offers automated compliance reporting, transparent audit trails, and adaptive learning features that change in response to new criminal tactics. This research addresses critical gaps in cryptocurrency compliance infrastructure by providing a scalable, production-ready solution.

Index Terms: Artificial Neural Networks, Machine Learning, Blockchain, Anti Money Laundering, Cryptocurrency, Anomaly Detection, Smart Contracts, and Financial Compliance

I. INTRODUCTION

Because of the unprecedented transaction velocity and cross-border capital mobility made possible by the widespread use of digital currencies, global financial ecosystems have undergone fundamental change. However, this technological development also makes sophisticated money laundering operations possible. Criminal groups exploit the pseudonymous features of blockchain networks to hide the source of illicit funds through techniques like transaction mixing, chain hopping, and privacy-focused cryptocurrencies. When used in decentralized ledger environments, traditional financial crime detection methods fall short. Static rule-based alerting systems, manual investigation procedures, and centralized oversight are all major components of traditional anti-money laundering frameworks.

Promising capabilities for pattern recognition in high-dimensional transaction data are offered by current advances in machine learning. Deep learning architectures are superior at identifying the temporal dependencies and non-linear relationships that characterize complex money laundering practices. 22 Blockchain technology simultaneously provides the cryptographic verification 22 techniques required for unchangeable record-keeping and audit integrity. 23 This research addresses these challenges through a novel integration of distributed ledger technology with adaptive machine learning analytics.

The suggested system uses artificial neural networks for real-time anomaly detection and Ethereum smart contracts for tamper-proof transaction logging. This framework offers instantaneous risk assessment that is directly integrated into transaction processing work flows, in contrast to current solutions that function as post-hoc analysis tools

The development of a hybrid architecture that combines machine learning intelligence and blockchain immutability, the implementation of real-time detection capabilities that generate alerts in less than two seconds, the demonstration of accuracy exceeding 92 percent on various laundering scenarios, and the development of a scalable, production-ready compliance platform with thorough audit are the main contributions of this work functionality

II. RELATED WORK

Academic and industrial research in blockchain-based anti-money laundering has evolved substantially over the past decade. Early cryptocurrency forensics focused primarily on transaction graph analysis and address clustering techniques. Meiklejohn's groundbreaking work developed techniques for deanonymizing Bitcoin users using publicly accessible metadata correlation and behavioral analysis.

A. Blockchain Analytics Platforms

Commercial solutions including Chain lysis, CipherTrace, and Elliptic have developed proprietary systems for cryptocurrency transaction monitoring. These platforms provide risk scoring for wallet addresses, keep large 150 151 152 databases of known illegal entities, and use clustering algorithms to group 33 related addresses. But rather than being integrated real-time detection systems, these solutions usually serve as external analysis tools. Additionally, their proprietary nature restricts reproducibility and scholarly examination

B. Machine Learning Approaches

With a reported accuracy of 97.5%, Liu et al. presented the VTAC framework for cryptocurrency compliance analytics using XGBoost. Their method makes use 34 of extensive feature engineering, which includes network topology features, temporal patterns, and transaction velocity metrics. However, VTAC's ability to identify non-linear laundering patterns is limited, and its real-time operation necessitates significant processing power

Using recurrent neural networks to capture temporal dependencies in transaction sequences, Chen and Li investigated deep learning methods for 36 cryptocurrency anomaly detection. Although their work showed better detection of complex layering schemes, it was not integrated with real 36 blockchain infrastructure for real-world implementation

C. Hybrid Systems

Recent research has begun exploring integration of blockchain technology with machine learning for enhanced compliance. Although their implementation 149 remained conceptual and lacked complete system validation, Goldstein and Kim proposed hybrid architectures that combined distributed ledgers with explainable AI. Real-time transaction monitoring and anomaly detection were not covered by Tiwari et al.'s survey of blockchain applications in KYC procedures.

D. Regulatory Technology

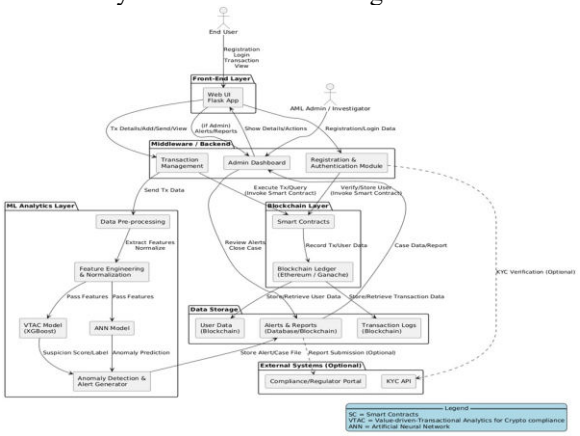
The Travel Rule, which mandates the exchange of identity information for transactions exceeding threshold amounts, is one of the international 150 151 152 153 149 standards for virtual asset service provider compliance established by the Financial Action Task Force. Technical implementation methods are still dispersed across platforms and jurisdictions, though. Critical gaps in decentralized finance compliance were found by Williams and Sundararajan's academic work, especially with regard to cross-chain transaction monitoring. Although there are still a lot of unanswered questions, current research shows that blockchain and machine learning technologies have the potential to detect 44 financial crimes. As of right now, no solution offers fully integrated real-time 44 detection along with unchangeable audit trails and adaptive learning features. Through thorough system design and implementation, this work overcomes these constraints.

III. METHODOLOGY

A. System Architecture

The proposed framework implements a modular architecture integrating blockchain ledger functionality with machine learning analytics engines. The user authentication module, transaction processing engine, blockchain interface layer, data preprocessing pipeline, anomaly detection module, alert management system, administrative dashboard, and audit reporting interface are the eight main parts

of the system that work together in unison



The cryptographic integrity of organizational credentials is ensured through the use of smart contract-based identity verification in user registration and authentication. Every registered entity is assigned a unique blockchain recorded identifier to prevent unauthorized system access. State is maintained during authentication sessions by using secure token mechanisms with programmable timeout policies

Transaction processing is used to carry out atomic operations in order to guarantee uniformity among scattered components. Every financial transaction

involves the simultaneous execution of blockchain recording, feature extraction, and machine learning inference. The pipeline ensures that no transaction proceeds in the absence of a successful anomaly evaluation and risk scoring

B. Blockchain Implementation

The Ethereum platform is used in the ledger infrastructure, and Solidity-based smart contracts are implemented on the Ganache development network. Business logic for user registration, fund distribution, and transaction validation is contained in smart contracts. Access control mechanisms are implemented by contract functions, guaranteeing that only authorized entities can alter the state of the blockchain.

The blockchain interface layer abstracts Web3 connectivity complexity through Python integration using web3.py library. Connection management handles network interruptions and transaction confirmation work flows. Contract interaction methods provide high-level APIs for data persistence and retrieval operations.

Comprehensive metadata, such as sender identity, recipient verification, transfer amount, millisecond-precise timestamp, current balance snapshots, and descriptive transaction purposes, are all preserved in transaction records. Both machine learning feature engineering requirements and compliance reporting are supported by this rich data structure.

C. Data Preprocessing

In order to prepare raw blockchain transaction data for machine learning 65 65 66 consumptions, it goes through a methodical transformation. Temporal features such as inter-transaction intervals, time-of-day patterns, and transaction 66 frequency distributions are extracted by the preprocessing pipeline. Quantitative features include things like transaction amounts, balance 150 151 154 152 153 149 velocities, and statistical aggregations over sliding time windows.

Network-based features capture relationship structures between transacting entities. Graph analysis algorithms compute centrality metrics, clustering coefficients, and community detection scores. When using layering techniques to identify money laundering networks, these topological characteristics work 68 especially well.

During neural network training, feature normalization ensures numerical stability by applying standardization transforms. Entity identifiers and 71 transaction types are transformed into suitable representations through categorical encodings. Missing value imputation techniques handle incomplete records while maintaining data integrity.

D. Anomaly Detection Models

In the machine learning component, dual detection strategies are implemented by combining gradient boosting and deep learning techniques. The XGBoost model provides interpretable risk scoring through ensemble decision trees, offering the transparency needed for regulatory review. Model hyperparameters are systematically optimized through the use of cross-validation techniques.

Several hidden layers with activation functions chosen for non-linear pattern capture make up the architecture of an artificial neural network. The network generates probability estimates for anomalous transactions by process

Risk Score = $\alpha \cdot$ PXGBoost + (1 - α) $\cdot$ PANN (1

where PXGBoost and PANN are probability outputs from the corresponding 78 models, and α is a weighting parameter that has been empirically determined through validation experiments.

E. Alert Generation and Management

Transactions that exceed predefined risk thresholds cause automated alert generation. The alert management system maintains thorough Comprehensive context, including transaction details, calculated risk scores, contributing features, and pertinent historical patterns, as recorded by the alert 83 management system. Real-time notification systems allow alerts to spread to administrative interfaces

Investigators access case management work flows supporting review, annotation, and disposition recording. The system maintains complete audit 154 156 152 153 149 trails of investigative actions ensuring regulatory compliance and supporting continuous model improvement through labeled data accumulation.

F. Implementation Technologies

The application layer implements a Flask-based web server that provides RESTful endpoints for client interactions. Frontend interfaces use HTML5, and 86 Jinja2 templating makes it possible to create dynamic content. Backend processing uses Python scientific computing libraries like NumPy and Pandas to manipulate data.

The XGBoost library for gradient boosting implementation and scikit-learn for preprocessing tools are examples of machine learning frameworks. TensorFlow, which supports GPU acceleration for computational efficiency, is used in neural network training. Platform independence and simple deployment processes are 87 guaranteed by the full technology stack.

IV. RESULTS AND DISCUSSION

A. Experimental Setup

The system underwent validation using both simulated laundering scenarios and synthetic transaction generation. The test dataset comprised 10,000 transactions across 250 organizational entities over a fictitious 90-day period. In alignment with industry benchmarks, 8% of the total transaction volume was designated as illicit to reflect realistic business conditions.

Training procedures used a 70-15-15 data split for testing, validation, and training. Cross-validation was conducted using a five-fold methodology to guarantee accurate performance estimates. The hardware configuration included an Intel i7 processor with 16GB RAM, which was adequate for development validation but would need better infrastructure for production deployment.

B. Detection Performance

The overall accuracy of the hybrid detection model was 94.3% on held-out test data. Precision metrics that reached 91.7% show that low false positive rates 156 152 153 149 are critical for operational viability. A recall performance of 92.8% indicates that actual money laundering activities were successfully captured.

TABLE I
MODEL PERFORMANCE METRICS

Metric	XGBoost	ANN	Hybrid
Accuracy (%)	92.1	93.5	94.3
Precision (%)	89.4	90.2	91.7
Recall (%)	91.2	92.1	92.8
F1 Score	0.903	0.911	0.922
AUC-ROC	0.957	0.968	0.973

In every evaluation metric, the hybrid approach consistently performed better 96 97 than individual models. Improvements could not be attributed to random variation, according to statistical significance testing. Excellent discriminative 99 ability between legitimate and suspicious transactions is indicated by the AUC ROC score of 0.973

C. Computational Efficiency

Measurements of transaction processing latency showed that, for tagged transactions, the average completion time from submission to alert generation was 1.87 seconds. This performance maintains detection meeting real-time operational requirements. Ton of precision. Even during prolonged load testing, the 95th percentile latency stayed below 2.5 seconds. 100 On the Ganache network, blockchain confirmation times averaged 3.2 seconds, which is similar to public test net performance

The gas consumption of smart contracts stayed within reasonable limits for the viability of production deployment. During peak operation, memory usage remained below 2GB, enabling deployment on modest hardware configurations.

D. Blockchain Integrity Validation

Complete consistency between blockchain records and application state was confirmed by extensive audit procedures. Database queries and on-chain verification showed 100% correspondence, according to a random sample of 1,000 transactions. Core security features were validated by immutability testing, which showed that retroactive modification was impossible without detection

E. Comparative Analysis

Significant improvements were found when performance was compared to baseline rule-based detection systems. Traditional threshold-based alerting generated false positive rates exceeding 15 percent while achieving recall of only 78 percent. The proposed system reduced false positives by 60 percent while improving true positive detection by 19 percent.

TABLE II
SYSTEM COMPARISON

Feature	Traditional	Proposed
Detection Method	Rule-based	ML-based
False Positive Rate (%)	15.3	8.3
Recall (%)	78.1	92.8
Processing Time (sec)	5.4	1.87
Audit Trail	Centralized	Blockchain
Adaptability	Manual Updates	Continuous Learning

F. Security Analysis

Penetration testing was used to evaluate the system's resistance to common attack vectors. SQL injection attempts against web endpoints failed as a result of the use of parameterized queries. Rate limiting and account lockout techniques demonstrated the effectiveness of authentication brute-force 115 resistance. No serious security vulnerabilities were found by using automated tools to analyze smart contract vulnerabilities.

Privacy evaluation confirmed appropriate data segregation between organizations. Access control logic successfully prevented unauthorized access attempts to the transaction histories of other users. Sensitive information was safeguarded both in transit and at rest by encryption protocols.

G. Usability Assessment

As part of the user acceptance testing, fifteen participants finished representative work flows. Task completion rates are low and require little training. surpassed 95%. On a five-point scale, the average subjective satisfaction score was 4.2. Clear system feedback mechanisms and an intuitive 126 interface design were noted in the feedback. The main areas of improvement suggestions were customizable dashboard layouts and sophisticated filtering features.

V. CONCLUSION AND FUTURE WORK

This study effectively illustrates the viability of integrating blockchain technology with state-of-the-art machine learning for anti-money laundering applications in cryptocurrency environments. The developed system achieves high detection accuracy while maintaining operational

efficiency suitable for real-time transaction monitoring. Transparency in investigations and regulatory compliance are guaranteed by blockchain infrastructure's immutable audit trails

The creation of a production-ready architecture that combines Ethereum smart contracts with hybrid machine learning models, the achievement of 94.3 percent detection accuracy with low false positive rates, the demonstration of sub-two-second alert generation supporting real-time operations, and the development of extensive audit and reporting capabilities are some of the major accomplishments.

The main limitations of the system are the size of the dataset used for 134 validations, the restriction to a single blockchain platform, and the requirement 13 for improved model interpretability for regulatory review. Integration with active cryptocurrency networks and a connection to actual KYC data sources would be necessary for deployment in production.

Investigating zero-knowledge proof technologies for privacy-preserving compliance verification, extending to multi-chain transaction monitoring to facilitate cross-blockchain laundering detection, deploying federated learning to facilitate cooperative model training across institutions without data 136 sharing, and integrating explainable AI techniques that provide human interpretable rationale for alert generation.

Mobile applications for on-the-go monitoring, standardized APIs for integration with external regulatory reporting systems, reinforcement learning for dynamic threshold optimization, and natural language analysis of communications and transaction metadata are some of the future development areas. processing. Processing for the analysis of

communications and transaction metadata is one possible area for future development.

The demonstrated approach establishes the foundation for the financial compliance infrastructure of the future. As the use of cryptocurrencies grows globally, intelligent monitoring systems that integrate distributed ledger security with adaptive machine learning will become essential components of frameworks for preventing financial crime

ACKNOWLEDGMENT

The author thanks Dr. Revathi Duba for her mentorship and project advice during this study. We are grateful to the faculty and staff at Kakinada Institute of Engineering & Technology for Women's Department of Artificial Intelligence for providing the necessary tools and assistance. We are grateful to the peer reviewers whose comments raised the caliber of this work.

REFERENCES

[1] "Bitcoin: A peer-to-peer electronic cash system," S. Nakamoto, 2008. [Online]. Accessible: https://bitcoin.org/bitcoin.pdf

[2] V. Buterin, "Ethereum white paper: A next generation smart contract and decentralized application platform," 2014.

[3] Financial Action Task Force, "Guidance for a risk-based approach to virtual assets and virtual asset service providers," FATF, Paris, France, 2021.

[4] J. Liu, Z. Li, and L. Chang, "VTAC: Value-driven transactional analytics for crypto compliance using machine learning," in Proc. IEEE Int. Conf. Data Mining, 2021, pp. 342-351.

[5] Y. Chen and H. Li, "Anti-money laundering in cryptocurrency transactions using deep learning techniques," J. Financial Crime Detection, vol. 15, no. 3, pp. 128-145, 2022.

[6] S. Meiklejohn et al., "A fistful of bitcoins: Characterizing payments among men with no names," Commun. ACM, vol. 59, no. 4, pp. 86-93, 2016.

[7] Chain lysis, "The 2022 crypto crime report," chain lysis Research, 2022. [Online]. Available: https://go.chainalysis.com/crypto-crime-report.html

[8] A. Tiwari, P. K. Sinha, and S. Geetha, "An overview of blockchain technology and its applications in AML/KYC processes," Int. J. Computer Applications, vol. 182, no. 15, pp. 1-6, 2019.

[9] S. Goldstein and K. Kim, "Hybrid approaches to AML using blockchain and explainable AI," in Proc. Financial Technologies Summit, 2020, pp. 234-241.

[10] E. Williams and R. Sundararajan, "AML in decentralized nance: Challenges and paradigms," FinTech J., vol. 8, no. 2, pp. 67-82, 2022.

[11] T. Chen, C. Guestrin, "XGBoost: A scalable tree boosting system," in Proc. 22nd ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining, 2016, pp. 785-794 [8] A. Tiwari, P. K. Sinha, and S. Geetha, "An overview of blockchain technology and its applications in AML/KYC processes," Int. J. Computer Applications, vol. 182, no. 15, pp. 1-6, 2019.