Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 10| 2025

Research Article **Received:** 05-09-2025| **Accepted:** 05-10-2025 | **Published:** 19-10-2025

AI and Machine Learning in Detecting Terrorist Financing Through Cryptocurrency in the U.S.

Oluwatosin Oladokun [1], Samuel Amfo Junior [2], and Jehu Emefa Nii-Laryea Laryea [3]

[1]*Haas School of Business, University of California, Berkeley, Berkeley, CA, USA*
[2]*Department of Computer and Information Technology, Eastern Illinois Technology, Illinois, USA*
[3]*Department of Business Administration, University of Professional Studies, Ghana*

Abstract: The rapid expansion of cryptocurrency has revolutionized financial transactions by enabling fast, decentralized, and borderless value transfer. While these innovations have created new economic opportunities, they have also introduced loopholes that can be exploited for illicit purposes, particularly terrorist financing. In the United States, authorities have shown concern about how digital currencies are being used to fund terrorism. Because blockchain transactions are hard to trace and often anonymous especially when tools like mixers and cross-chain swaps are involved, traditional systems struggle to keep up. This study explores the role of Artificial Intelligence (AI) and Machine Learning (ML) in detecting terrorist financing through cryptocurrency within the U.S. context. By employing advanced techniques such as anomaly detection, graph neural networks, and ensemble learning, AI/ML models can analyze transaction patterns at scale, identify hidden relationships, and improve the accuracy of suspicious activity detection. The research integrates insights from blockchain analytics, regulatory frameworks, and compliance practices to assess both technical and institutional factors influencing detection effectiveness.

Keywords: Cryptocurrency, Terrorist Financing, Artificial Intelligence, Machine Learning, Blockchain Analytics.

INTRODUCTION

Cryptocurrency is a digital currency that operates without the need for a central bank or financial institution to verify transactions. The rapid evolution of cryptocurrency platforms has fundamentally changed the global financial system by introducing new paradigms for conducting and recording transactions. These are purely digital assets or currency verified and recorded using blockchain technology, offer secure and anonymous methods for transferring value. Cryptocurrencies such as Bitcoin, Ethereum, and Monero provide fast, borderless and decentralized transactions (Härdle, Harvey, & Reule, 2020; Jaiswal & Chaudhari, 2023).

While these innovations have provided significant economic opportunities, they have also introduced unprecedented risks for illicit finance, including terrorist financing (Agorbia-Atta, Atalor, Agyei, & Nachinaba, 2024). Terrorist financing involves the means and methods used by terrorist organizations to finance their activities. This money can come from legitimate sources, for example from business profits and charitable organizations, or from illegal activities including trafficking in weapons, drugs or people, or kidnapping (United Nations Office on Drugs and Crime, 2024).

In the United States, regulators such as the Financial Crimes Enforcement Network, the Office of Foreign Assets Control and law enforcement agencies are increasingly concerned about the misuse of cryptocurrencies for terrorism-related activities. The challenge lies in the complexity of blockchain transactions where pseudonymity, mixers, peel chains, and cross-chain swaps hinder effective monitoring. Although blockchain is inherently transparent, the vast scale of data and the sophisticated methods employed by illicit actors make manual detection insufficient (Wang & Zhu, 2021).

Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful tools to address this gap. By analyzing transaction graphs, identifying anomalies and learning from past enforcement data, these systems can help detect suspicious activity that might otherwise go unnoticed. Techniques such as graph neural networks, anomaly detection, and ensemble learning offer new opportunities to enhance Anti-Money Laundering and Counter-Terrorist Financing frameworks. Moreover, integrating AI and ML with blockchain analytics tools has opened new avenues for tracing and disrupting illicit financial flows within cryptocurrency networks.

LITERATURE REVIEW

Terrorist Financing and Cryptocurrencies

Terrorist financing refers to the methods by which terrorist groups raise, store, and move funds to support their operations. Traditionally, terrorist financiers primarily relied on the banking system

***Corresponding Author:** Oluwatosin Oladokun

DOI- https://doi.org/10.5281/zenodo.17390521

and employed methods such as foreign shell companies, money transfers, Hawala systems, and high-value commodities (Jofre, Aziani, & Villa, 2024**)**. However, with the rise of digital assets, terrorist groups are increasingly exploring cryptocurrencies as a means of raising and transferring funds. The decentralized, pseudonymous, and borderless characteristics of cryptocurrencies present both opportunities and risks.

Fanusie and Robinson (2018) argue that while the scale of terrorist use of cryptocurrency remains relatively small compared to traditional methods, the potential for growth exists, particularly as blockchain technology adoption becomes more widespread.

In response to these threats, U.S. agencies such as the Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC) have imposed sanctions and compliance obligations on virtual asset service providers (VASPs). FinCEN's 2021 priorities emphasize the need to monitor digital asset transactions and enhance cross-border cooperation. However, issues related to cross-border jurisdiction and the lack of standardized global regulations have made these enforcements challenging.

The integration of Artificial Intelligence (AI) and Machine Learning (ML) within cryptocurrency ecosystems has significantly enhanced financial surveillance and illicit activity detection. AI/ML models particularly decision trees and neural networks can achieve precision and recall rates exceeding 90% when analyzing large-scale blockchain data to identify illicit flows (Agorbia-Atta et al. 2024). These results highlight the capability of AI/ML to improve Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) systems.

BACKGROUND AND REGULATORY FRAMEWORK

Terrorism has long been threatening national security, life and property of nations around the world. Since the September 11 attack, terrorism has become a central focus of international policy and to eliminate this requires a long-term effort.

Cryptocurrencies, particularly Bitcoin and other blockchain-based digital assets, have transformed financial systems by enabling decentralized, peer-to-peer transactions without intermediaries. While they offer benefits such as financial inclusion, faster cross-border payments, and enhanced privacy, they also pose risks for illicit activities like money laundering and terrorist financing.

To address these concerns, the United States has developed a robust regulatory and enforcement framework aimed at combating illicit use of cryptocurrencies, especially in the context of terrorist financing. These regulators include Bank Secrecy Act (BSA), Anti-Money Laundering (AML) rules, and agencies such as Financial Crimes Enforcement Network (FinCEN), Securities and Exchange Commission (SEC), Office of Foreign Assets Control (OFAC) and Commodity Futures Trading Commission (CFTC) (Wang & Zhu, 2021).

These agencies coordinate efforts to detect, deter, and disrupt the illicit use of digital assets. FinCEN requires virtual asset service providers (VASPs) to implement Know Your Customer (KYC) procedures and report suspicious activity. OFAC imposes sanctions on individuals and entities associated with terrorism, including those using cryptocurrencies for fundraising.

Despite this progress, challenges related to regulation and enforcement remain. The global nature of cryptocurrency transactions complicates jurisdictional monitoring, and the lack of standardized international regulations creates loopholes that illicit actors can exploit. These challenges make the integration of advanced technologies such as AI and ML even more essential in enhancing national and global financial security.

METHODOLOGY

Research Design

This study employs a qualitative methods design, combining documentary analysis and case study analysis to explore the role of Artificial Intelligence and Machine Learning in detecting terrorist financing through cryptocurrency in the United States. This approach ensures a comprehensive understanding of both the technical and institutional dimensions of the issue.

Data Collection Methods

Secondary Data (Documentary Review): Academic journals, government reports, and policy papers from agencies such as the Financial Crimes Enforcement Network (FinCEN), Office of Foreign Assets Control (OFAC), and U.S. Treasury will be analyzed. Reports from blockchain analytics firms (e.g., Chainalysis, Elliptic, CipherTrace) provide insights into

Publisher: SARC Publisher

patterns of enforcement, technical challenges and regulatory gaps. To identify existing AI/ML applications in crypto AML/CFT.

Case Study Selection

Two exploratory case studies were selected to examine real-world enforcement actions involving cryptocurrency-based terrorist financing**:**

- Case 1: U.S. Department of Justice seizure of ISIS-linked wallets (2020), involving darknet and social media fundraising.
- Case 2: OFAC sanctions against Hamas-affiliated wallets (2022), using blockchain-based donations.
- Cases were chosen for their public availability, technical details, and institutional response, as well as for their illustrative use of AI-enabled analytics during investigation or compliance processes.

FINDINGS

Increasing Use of Cryptocurrency by Terrorist Groups:

Evidence shows that terrorist organizations are experimenting with cryptocurrency to bypass traditional financial controls. Case studies from the U.S. Department of Justice (DOJ) and the Office of Foreign Assets Control (OFAC) reveal that terrorist groups such as Hamas and ISIS have used Bitcoin and other cryptocurrencies to raise funds, often leveraging social media and darknet platforms (Fanusie & Robinson, 2018; OFAC, 2022). While the overall volume remains small compared to traditional methods, the trend is growing due to the accessibility and borderless nature of digital assets.

Effectiveness of AI and Machine Learning in Detection:

Artificial intelligence (AI) and machine learning (ML) techniques have proven highly effective in detecting suspicious cryptocurrency transactions. Methods such as graph-based anomaly detection, supervised learning, and neural networks have been used to identify illicit wallet addresses and transaction patterns associated with terrorist financing. Additionally, blockchain analytics firms like Chainalysis and Elliptic utilize AI-powered tools to uncover hidden networks and trace complex transaction flows involving mixers and peel chains (Agorbia-Atta, Atalor, Agyei, & Nachinaba, 2024; Pocher *et al.*, 2023).

Regulatory and Institutional Challenges:

Despite technological progress, regulatory and institutional gaps hinder effective adoption of AI/ML tools. Agencies like FinCEN and OFAC have imposed sanctions and compliance obligations on virtual asset service providers, but enforcement faces difficulties due to cross-border jurisdictional issues and lack of standardized regulations (FinCEN, 2021). Additionally, the explainability problem in AI models raises concerns for regulators, who require transparent justifications for enforcement decisions (Bryman, 2016).

DISCUSSION

The findings highlight the dual challenge of innovation and risk, while cryptocurrency provides terrorists with new opportunities for funding, Artificial Intelligence and Machine Learning present equally powerful opportunities for detection. The use of graph neural networks and anomaly detection models demonstrates that AI can significantly improve detection accuracy compared to manual methods (Zeng *et al.*, 2021). These models can uncover hidden links within massive blockchain datasets, making it possible to identify clusters of wallets associated with illicit activity.

However, the success of AI depends heavily on data availability and regulatory alignment. Without standardized reporting across exchanges and international cooperation, terrorist networks can exploit regulatory loopholes. Moreover, the “black box” nature of AI models remains problematic. Regulators and courts require explainable results to ensure fair enforcement, yet many ML algorithms lack transparency (Rehman *et al.*, 2020). This limits adoption despite technical potential.

Another significant issue is adversarial adaptation: as AI systems improve, terrorist networks may employ more advanced obfuscation techniques such as privacy coins (e.g., Monero, Zcash) and decentralized exchanges to evade detection. These dynamic underscores the need for continuous innovation and collaboration among regulators, AI researchers, and blockchain analytics firms.

Overall, the discussion suggests that AI and ML are not standalone solutions, but integral components of a broader framework that combines technology, regulation, and human expertise. The U.S. must strengthen public private partnerships, invest in explainable AI research, and expand international cooperation to fully leverage Artificial Intelligence and Machine Learning against cryptocurrency-based terrorist financing.

Publisher: SARC Publisher

CONCLUSION AND RECOMMENDATIONS

Conclusion

This research examined the application of Artificial Intelligence and Machine Learning in detecting terrorist financing through cryptocurrency within the United States. The findings indicate that while terrorist groups' reliance on cryptocurrency remains relatively limited compared to traditional funding methods, the growing sophistication of digital assets presents an evolving threat to national security.

Artificial intelligence and Machine Learning tools have demonstrated significant potential in identifying illicit flows across blockchain networks by applying anomaly detection, graph analysis, and predictive modeling. These techniques enhance the effectiveness of Anti-Money Laundering and Counter-Terrorist Financing frameworks by enabling regulators and financial institutions to analyze vast and complex transaction data.

However, the study also highlighted challenges such as regulatory fragmentation, limited adoption by smaller institutions, and the opacity of certain AI models. Moreover, the dynamic nature of adversarial techniques such as the use of privacy coins, mixers, and decentralized exchanges requires continuous innovation in detection methods.

Recommendations

Enhance Regulatory Harmonization:
The U.S. should strengthen coordination between agencies such as FinCEN, OFAC, and the Securities and Exchange Commission (SEC) to create a unified regulatory framework.International collaboration should be expanded through bodies like the Financial Action Task Force (FATF) to address cross-border risks.

Invest in Explainable AI Research:
To increase trust and accountability, AI systems used in detecting illicit transactions should prioritize explainability, ensuring regulators can justify enforcement actions.

Expand Public-Private Partnerships:
Financial institutions, blockchain analytics firms, and regulators should engage in greater information sharing to enable real-time threat detection and facilitate the deployment of cutting-edge AI/ML tools.

Support Capacity Building for Smaller Institutions:
Smaller banks and financial service providers should receive technical support, training, and subsidized access to AI-based compliance tools to ensure broad adoption of detection systems.

REFERENCES

1. Härdle, W. K., Harvey, C. R., & Reule, R. C. "Understanding cryptocurrencies." *Journal of Financial Econometrics* 18.2 (2020): 181-208.
2. Jaiswal, V. K., & Chaudhari, A. K. "Cryptocurrencies: Evolution, challenges, and future prospects." *Journal of Software Engineering and Simulation,* (2023).
3. Agorbia-Atta, C., Atalor, I., & andRichard Nachinaba, R. K. A. "Combating terrorist financing in cryptocurrency platforms: The role of AI and machine learning." *World Journal of Advanced Research and Reviews* 23.3 (2024): 1477-1486.
4. United Nations Office on Drugs and Crime, "countering the financing of terrorism." (2024):
5. Wang, S., & Zhu, X. "Evaluation of potential cryptocurrency development ability in terrorist financing." *Policing: A Journal of Policy and Practice* 15.4 (2021): 2329-2340.
6. Fanusie, Y. J., Robinson, T., Fanuise, Y. J., & Robinson, T. "Bitcoin laundering: an analysis of illicit flows into digital currency services| Foundation for Defense of Democracies." *Fdd. Org* (2018).
7. Office of Foreign Assets Control (OFAC). "Sanctions advisory for the virtual currency industry. U.S. Department of the Treasury." (2022).
8. Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M. Z., & Ferretti, S. "Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics." *Electronic Markets* 33.1 (2023): 37.
9. FinCEN. "Anti-money laundering and counter-terrorist financing priorities. U.S. Department of the Treasury." (2021). https://www.fincen.gov/sites/default/files/shared/AML_CFT_Priorities.pdf
10. Bryman, A. "Social research methods. Oxford university press." (2016).
11. Jofre, M., Aziani, A., & Villa, E. "Terrorist Financing: Traditional vs. Emerging Financial Technologies." *Terrorism and Political Violence* (2024): 1-14.

Publisher: SARC Publisher

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Oladokun, O., Junior, S. A., and Nii-Laryea Laryea, J. E. " AI and Machine Learning in Detecting Terrorist Financing Through Cryptocurrency in the U.S.." *Sarcouncil Journal of Engineering and Computer Sciences* 4.10 (2025): pp 186-190.

Publisher: SARC Publisher