Combating Digital Money Laundering: Criminal Law Perspectives on Blockchain-Based Financial Systems

Dr. Indra Daman Tiwari[1], Dr. Yaman Kasturi[2], Deeba Ashraf[3], Navneet Yadav[4], Mr. Sourabh Batar[5]

[1]Assistant Professor, School of Law, T.S. Mishra University, Lucknow, Uttar Pradesh.
shivatiwari.lu@gmail.com

[2]Faculty of Law, Jamia Millia Islamia, New Delhi.
Yamankasturi15@gmail.com

[3]Legal Consultant, Law Commission of India, Ministry of Law & Justice, Government of India.
ddeebaashraf@gmail.com

[4]Legal Consultant, Law Commission of India, Research Scholar, Faculty of Law, Maharaja Surajmal Brij University, Kumher, Bharatpur.
yadav.navneet4rights@gmail.com

[5]Assistant Professor, TMCLLS, Teerthanker Mahaveer University, Moradabad.
battarsourabh@gmail.com

Abstract

This essay is a critical review of the emerging trends in cyber money laundering in blockchain based financial systems and how the criminal statutes are carefully dealing with the challenges. It explains the dynamics of the illegal laundering schemes used by criminal groups to conceal the origin of funds through the cryptocurrencies and distributed ledgers and analyses the threats that the new technologies have on the financial regulatory system. It further explores how the same innovations can be used by responsible authorities to enhance the transparency of financial transactions of criminals and ensure that the battle against money laundering and financing of terrorism is enhanced by the pursuit of such innovations. The very premise of cryptocurrencies the engine of innovation and an opening that allows criminals to thrive demands a comprehensive review of both legal and technological responses to criminal activities to reduce the projected 20-billion dust of dirty money exchanged in 2023. This paper, therefore, argues that an integrated strategy, involving sophisticated blockchain analytics and responsive legal and regulatory frameworks, is crucial to combat the obfuscation techniques commonly used in cryptocurrency-based financial offences. This review outlines the complexities of this integrated approach, including the status and admissibility of electronic currencies as evidence in money laundering investigations and, especially, in jurisdictions grappling with the infancy of these crimes. In particular, the absence of specific regulatory considerations for cryptocurrencies as evidence in criminal procedure codes (including those dedicated to money laundering investigations and prosecutions) presents challenges for law enforcement and prosecution.

Keywords:- Digital money laundering, blockchain, cryptocurrency, criminal law, anti-money laundering, financial crime, evidentiary challenges.

1. Introduction

The advent of blockchain technologies and cryptocurrency assets has brought new challenges to the global financial system, requiring a reappraisal of traditional anti-money laundering and counter-financing of terrorism measures. Although blockchain technologies provide unparalleled advantages, they also create new opportunities for sophisticated financial crime and, in this way, add to the complexities of tracing and interdicting illicitly sourced funds. The technological structure of some cryptocurrency assets, the decentralised nature of blockchain systems and the emergence of decentralised financial platforms (DeFi) hinder law enforcement efforts to track and trace illicit transactions. This is compounded by the international and often anonymous nature of cryptocurrency transactions, often exploiting jurisdictional loopholes and sophisticated mixing techniques such as "chain-hopping" and mixers to evade scrutiny. Despite these sophisticated concealment strategies, the inherent immutability and decentralised nature of blockchain technology inherently provides a level of transparency and traceability that can, in theory,

be harnessed for improved forensic investigations, contrary to popular belief that all cryptocurrencies are untraceable [1]. Nonetheless, drugs and inducements such as mixers, tumblers and privacy wallets only foil the sheer transparency because it is deliberate to obfy and conceal the original origin of the transactions to prevent police detection of illegal transactions in the battle against the money laundering of the bank deposit of the locals as opposed to the funding of terrorism activities (AML/CFT). This will require high levels of multidisciplinary alternatives to combine legal and technological limits in studying the forensic strategies of hugging close and making inroads into the illicit financial transfers in these newfound digital financial framework. In this connection, there should be a critical analysis of how the law in the criminal law limits the underlying difficulties of combating the digital money laundering in blockchain-based financial systems, with particular reference being made to the process of providing meaningful regulatory and enforcement arrangements. Since the cryptocurrency systems are decentralised and anonymous and are vulnerable to cyberattacks, they are considered a major risk in the misuse of the cryptocurrency in money laundering and the funding of terrorist activities [2].

2. The Evolution of Digital Money Laundering

The anonymous and decentralized nature of cryptocurrencies and more importantly the rise of unregulated commercial activities and cross-border opportunities has provided multitudes more options on the presence of undermining evil money and relegated the traditional money laundering schemes. Various types of ways of hiding the source and identity of illegitimate funds are being embraced by criminal groups, e.g., chain hopping, mixers etc. The concealing cryptocurrencies of such techniques like Monero and Zcash further make it difficult to follow the trail of the finances using the information in the transactions and the identity of the senders and receivers in the transactional records, to various law enforcement agencies [3]. However, the fundamentals of money laundering, placement, layering and integration, still have the conceptual same foundation, even when applied to currencies based on blockchains.

The principles have not changed, yet the technological advances of digital assets present new difficulties in locating and stopping these steps and, more specifically, through the layering process, where instantaneous and international deals and smart contracts may be used to construct complex audit trails. The very specifics of the electronic currency, which is only in its electronic form, necessitate particular legal considerations, such as the separation it forms when compared to other types of electronic information with regard to its evidentiary value in legal case. The rise of blockchain and the advent of digital assets has changed the nature of financial transactions, presenting an efficiency and regulation challenge. Specifically, cryptocurrencies have enhanced the lifecycle of thousands of cybercrimes, particularly ransomware, identity theft, and selling of digital goods by making them anonymous and decentralised. The anonymity in transactions in which a user will be able to execute transactions without revealing their identity and the lack of a central authority to regulate transactions gives this space a perfect breeding ground to develop sophisticated money laundering methods. Moreover, the convergence of cryptocurrencies and the dark web has made the problem even worse, since criminals can now sell illegal goods and services anonymously, purchasing virtual currencies, which are later laundered to cover the proceeds [4].

Virtual currencies used in standard financial operations also contribute to the difficulty as it becomes hard to differentiate between a genuine and a criminal financial transaction that makes the task of identifying a money laundering scheme more complex. The operation of tracing transactions that may take a variety of networks on such blockchains, especially when such blockchains are based on privacy-oriented digital currencies, becomes a challenge to the work of financial intelligence services and law enforcement to identify and divert the works of money laundering. This requires high-level tracing tools and international cooperation sites to eliminate territorial issues and computer cloaking muzzles utilized by the criminal group. It is also complicated by the fact that the transactions are international, where globalizing regulations and

global customs to fight off online money-laundering needs the international system to work together to address the problem. The seamless merging of technology and finance has also helped create the changes in the money laundering schemes too and have made them hard to track down and stop. Both this advancement demands the steady alteration in the means of regulation and the inquiry procedures in order to be aligned with the new and innovative strategies implemented in the online space.

3. Blockchain Technology and its Implications for Illicit Finance

Even though the blockchain as a ledger provides unquestionable clarity in the case of legitimate transactions as it is immutable and distributed, anonymity and international nature of the blockchain is another possible source of money laundering. In particular, the decentralisation of blockchain networks disorient the traditional financial monitoring systems, offering a chance to move illegal funds across the boundaries with little oversight. It is a slippery slope, where it is the technologies that assure safety and performance to make money laundered and conceal the origin and destination of illicit funds.

3.1. Fundamentals of Blockchain Technology

In principle, blockchain is a decentralised, resistant to tampering, registry of transactions stored in many computers. A block refers to a group of transactions hashed (cryptographically secured) and connected to the last block, which offers integrity and order. This cryptographic chaining makes it extremely difficult to tamper with historical transactions, thus offering a secure method of maintaining records. This immutability, which is advantageous for transparency, also introduces forensic challenges when criminal activities are infused into the blockchain, requiring sophisticated methods to unmask transactions and trace funds [5]. Additionally, the decentralised nature of many blockchain systems poses challenges for enforcement authorities who may not know who to request data from or seize assets from, and therefore may need to work across borders and have bespoke legal frameworks to overcome jurisdictional issues.

3.2. Anonymity and Pseudo-anonymity in Blockchain Transactions

Although the addresses used for blockchain transactions are pseudo-anonymous, allowing for some level of privacy, this also makes it difficult to directly connect on-chain transactions to real-world identities. This pseudo-anonymity, where transaction data is public but user identities are hidden, both increases privacy for legitimate users, and makes illicit activities more appealing, as the users are hidden. This complicates the execution of anti-money laundering measures, as Know Your Customer and Customer Identification Procedures cannot easily be executed. But increasingly, blockchain forensic techniques and analysis tools are being used to "unmask" transactions by tracking the movement of funds and grouping addresses that might be linked to a particular entity or illegal activities. This includes advanced clustering techniques, heuristic-based analyses and other methods to detect connections and patterns that could expose underlying real-world identities and their financial networks[6].

3.3. Decentralization and Cross-Border Challenges

The peer-to-peer nature of blockchain transactions, while increasing efficiency and lowering costs, also bypasses regulatory scrutiny that typically exists in financial transactions. This lack of a governing authority, combined with the borderless nature of many blockchain networks, presents numerous jurisdictional challenges for regulatory agencies and law enforcement authorities involved in tackling illicit activities. In particular, the borderless nature of these networks enables criminals to make cross-border transfers and conversions of illicit funds, which are difficult to track and recover by national regulatory bodies [7].

Such uncertainty in jurisdiction is further complicated by the country to country differences in the law and it becomes difficult to know which country to apply the law of a cryptocurrency transaction that cuts across borders.

4. Current Legal Frameworks and Their Applicability

The advent of financial networks based on blockchain technology necessitates the thorough reevaluation of the existing law and regulatory instruments to ascertain their efficiency in addressing the problems of digital money laundering. The decentralized blockchain ecosystems, whose pseudo-anonymity challenges the traditional financial intermediaries-oriented Anti-Money laundering and Know Your Customer laws.

4.1. International Anti-Money Laundering (AML) Standards

Financial Action Task Force has issued the guidelines to adapt AML/CFT requirements to the virtual asset service providers aiming at bringing these entities to the international framework and eradicate the cross-border risks related to the transfer of virtual assets. However, use and implementation of these rules varies across nations, which allows regulatory arbitrage and misuse by malicious individuals to launder money. Also, the difference in national strategies on the regulation of blockchain between specific legislation and the adjustment of the current financial regulations contributes to the cross-border regulatory problems and worldwide regulatory complexity as well. This will allow rogue players to take advantage of these regulatory loopholes by registering their business in jurisdictions with laxer regulatory controls, thus compromising the work of the global AML regulatory structure.

4.2. National Criminal Law Responses to Digital Money Laundering

The nations have reacted to these concerns by adopting certain legislations and restructuring their criminal legislations to cover virtual assets, but it remains questionable and is reliant on the dynamic blockchain experience. As an example, in the US, cryptocurrency exchanges are considered to be Money Services Business by the Financial Crimes Enforcement Network, subjected to the compliance with the Bank Secrecy Act, including effective Know Your Customer and Anti-Money launder and other requirements, yet their enforcement is inconsistent across different states. In the meantime, most jurisdictions have demonstrated non-compliance or partial compliance with the FATF requirements on virtual assets, leading to a fragmented and sometimes ineffective global legal framework of cryptocurrency.

4.3. Jurisdictional Issues and Enforcement Challenges

Due to the international character of blockchain, as well as the decentralisation of the management of virtual resources, the jurisdiction problem may appear, making it more difficult to prosecute and seize unlawful funds. This is especially so where cross boundaries and jurisdiction are being applied in illicit transactions and these jurisdictions are in different legal definitions and implementation of the law on digital assets. This imbalance of the regulations system in different jurisdictions allows criminal activities to enjoy a small arbitrage of jurisdiction where the actual criminal activity can be transferred to jurisdictions with more relaxed regulatory systems. Also the cross-regional differences in how regulatory frameworks are applied and enforced worldwide such as the FATF Travel Rule is also an issue that has been repeated in combating money laundering based on cryptocurrency use and only a minor fraction of implementing jurisdictions have made efforts to enforce such measures [8]. This brings to the fore the reality that the global regulatory and legal frameworks are yet to agree on the best way to assist in curbing global digital money laundering, but far more important is to ensure that application of laws can be harmonized across the world.

5. Challenges in Applying Criminal Law to Blockchain-Based Systems

The regulatory measures notwithstanding, criminology still faces the technical peculiarities of blockchain as a challenge, especially when it comes to the identification and prosecution of unlawful activities. As an illustration, blockchain transactions are relatively anonymous, and as a result, they offer some level of privacy, yet they also make it difficult to trace the origin of illicit financial deals to individuals or entities, which complicates forensic investigation and legal prosecution.

5.1. Identification and Attribution of Offenders

Moreover, the anonymity issue is exacerbated by the fact that following the money throughout several blockchain networks and decentralised hubs may be complex because limited interoperability and transaction obfuscation (through mixers and tumblers) can cancel the trace of funds. Also, the use of privacy-oriented cryptocurrencies, including Monero and Zcash, which use advanced cryptography schemes to hide details about a specific transaction, makes it practically impossible to track money or identify users. Such online camouflage can even demand sophisticated forensic tools and expertise that is not available in many police agencies. Such difficulties are aggravated by the constantly changing nature of the obfuscation techniques, including cross-chain money laundering and the exploitation of the use of decentralized finance (DeFi)-oriented systems that is faster than law enforcement and regulatory efforts.

5.2. Evidentiary Challenges in Blockchain Forensics

Although the distributed and immutable ledger provides a transparency audit trail, it presents a complication to evidence admissibility and understanding; particularly to courts unfamiliar with cryptographic evidence and digital signed evidence. The decentralized and unidentified quality (commonly through the use of obfuscation techniques like mixers) of data stored on the blockchain also complicates forensic analysis since it is hard to determine users and sources of transactions. Moreover, lack of standardized methodology to blockchain forensics, and inability to connect blockchain evidence with real-life identities present significant challenges to offering admissible evidence in a court. This necessitates the use of improved blockchain forensic tools, information, which can provide real-time information on more than one blockchain network and use superior data analytics to tackle the problem of handling and analysing vast amounts of transactions. Law enforcement is still struggling with combating financial crime by monitoring, prosecuting and other cryptocurrency transactions due to the decentralized and non-traceable nature of cryptocurrency transactions.

5.3. Defining Criminality in Decentralized Autonomous Organizations (DAOs)

The Decentralized Autonomous Organizations phenomenon is introducing new issues to the criminal law since it lacks a legal entity and corporate governance framework, and it is more difficult to assign criminal responsibility to the actions of the DAO. The same can be said of the question of accountability of illicit transactions made possible by smart contracts in a DAO since shared and often anonymous contributions of a DAO make pinpointing responsibility difficult. Also, the automated quality of smart contracts in DAOs, though it is supposed to encourage transparency, has the unintended side effect of enabling illicit financial transactions to happen without human mediation, making it harder to attribute legal responsibility in the resulting case and spawning new methods of distributing criminal liability within a DAO.

6. Proactive Measures and Regulatory Innovations

Blockchain forensics presents challenges, together with the continuous change in the world of decentralized finance, demands a fluid legal and forensic practice to suitibly blame criminal intent and culpability in these novel organisms of association. The solutions to these threats require an interdisciplinary approach, consisting of a comprehensive regulatory framework, its more active international collaboration and further improvement of advanced forensic instruments to adequately suppress digital money laundering and cybercrime.

6.1. Know Your Customer (KYC) and Anti-Money Laundering (AML) Compliance in Digital Asset Services

Governments are also adopting proactive regulation in consideration of the ever-changing dynamism of cryptocurrency technologies, which in most instances, some of which governments are unable to mitigate. These involve proactive measures like developing superior blockchain surveillance products, which is an AI and machine learning product that analyzes transactional activity and draws probable instances of money laundering and numerous other crimes. They are particularly

important in the context of researching financial crime with the background of the anonymity of the cryptocurrency payments as a transnational phenomenon [10].

6.2. Regulatory Sandboxes and Innovation Hubs

A better KYC/AML strategy should be employed to assist virtual asset service providers to keep combating endemic attempts to use blockchain systems to perpetrate financial crime by performing intricate identity verification and monitoring of transfers. It is especially difficult in the decentralised model of the majority of blockchain applications, such as peer-to-peer transactions, where Virtual Asset Service Providers are absent and interaction with DeFi protocols, where there are no gatekeeping and oversight mechanisms. This has in turn led to a regulatory imperative that these new financial ecosystems must be of a certain degree of scrutiny and need not in effect necessarily throttle innovation; a security/growth equilibrium. New regulatory paradigms have thus been created in which they apply methods of data analytics and machine learning to identify potential suspicious pattern of transaction and illegal dealings in various blockchain environments.

6.3. International Cooperation and Information Sharing

Regulatory sandboxes give controlled assistance to companies to explore new blockchain products without the baking regulation of regulators and helps co-evolve in the model of compliance and technological advancements. The reason is that these programs create a feedback mechanism between the developers of the technology and the regulators in such a way that effective response to the challenge of anti-money laundering and counter-funding will be co-evolved and exploit the peculiarities of distributed ledger technologies. Such collaborating ground is especially important in the development of regulatory approaches that are likely to contribute to combating emerging threat, yet they ought to ensure the safe and legal application of blockchain technologies in the financial industry. The symbiotic relationship must be responsive and powerful enough to combat superior established and developed forms of

financial illicit activities, especially in the new and more diverse world of decentralized finance.

7. Technological Solutions for Combating Digital Money Laundering

Decentralization of blockchain transactions means that extensive international collaboration and good information exchange between jurisdictions is necessary to adequately address cross-jurisdictional cross-national digital money laundering and regulatory arbitrage. Such cooperation is vitally important in establishing common procedures of regulatory specific methods and enforcement controls in curbing regulatory arbitrage. Besides, information-sharing systems and multilateral deals can be established, and this aspect permits tracing illegal finances across the entire world and addressing advanced cyber-crime activities in other regulatory fields. This especially applies in the achievement of the Financial Intelligence Unit as being more effective in the prevention and detection of more sophisticated money laundering networks that utilize the world cryptocurrency networks [11].

7.1. Blockchain Analytics and Tracing Tools

The application of technologies that involve artificial intelligence, machine learning and high-order blockchain analytics plays a significant role in increasing the efficacy of identifying and curbing unlawful monetary activities. The technologies allow detecting complex money laundering transactions, such as those involved in concealing money through numerous crypto wallets or decentralized exchange, by means of main datasets that scan behaviors and patterns of anomalies [12].

7.2. Artificial Intelligence and Machine Learning in AML

The tools of analysis are specifically created to slice through the perceived anonymity of blockchain transactions, providing solutions to trace the funds used in a forensic way and identify the involved organizations. These tools can be used to re-identify wallet addresses and improve tracing of illicit funds through multiple blockchain networks and, thereby, support law enforcement agencies in breaking down criminal networks

through the use of the graph theory and clustering techniques. Many sources of data, including the open blockchain records and secret sources of intelligence, are combined with these analytical instruments to give a holistic view of illegal activity. In addition, Financial Intelligence Units have had the highest take-up of AI-based transaction monitoring, but there are significant disparities in the analytical performance of mature and immature Financial Intelligence Units [13].

7.3. Privacy-Enhancing Technologies and Their Dual Use

Not only do these technologies provide enormous gains to user privacy, but With its obfuscation capabilities, they can be used by criminals to hide illegal deals, potentially causing a serious threat to regulatory compliance and law enforcement efforts. This involves the development of non-invasive analytical techniques capable of identifying legitimate privacy-defending operations and those that are attempting to protect the obscurity of criminal financial operations, and the encouragement of accountable privacy-enhancement innovations [14]. In that manner, the policy conditions need to foster the emergence of privacy-saving techs without necessarily making them the channels of money laundering.

8. Conclusion

Overall, the battle against the digital money laundering needs to have a multi-pronged focus which presupposes the combination of both efficient regulation and advanced technology. Such a complex relationship is vital in the global fight against financial crimes within the context of the ever-evolving technologies, including blockchain and artificial intelligence (AI). This will entail a vibrant and collaborative approach by international regulatory authorities, financial institutions and technology providers that will address the challenges of integrity upholding the financial system in the face of new threats. And the ongoing technological innovation in the field of anti-money laundering, including regulatory technology and compliance automation, is vital for financial institutions to respond rapidly to changing risks and regulatory landscapes, and to maintain the effectiveness and resilience of anti-money

laundering systems. The symbiotic relationship between blockchain and machine learning, for example, is an effective approach to improving the accuracy and efficiency of AML initiatives. Yet the impact of some RegTech solutions in strengthening AML systems has been proven to be minimal, suggesting the need for a holistic approach that balances AML and privacy concerns by harnessing privacy-enhancing technologies. Thus, research should be directed towards advanced approaches to harness privacy-preserving artificial intelligence to enhance the monitoring of financial transactions while ensuring high levels of data protection. Moreover, the rapidly changing environment of blockchain-based financial systems calls for a flexible regulatory framework that balances the indisputable transparency of distributed ledgers with pseudonymous transactions exploited by criminals. Light-speedy financial innovation, which in many cases opens up more chances to another set of crooks, should also be considered in this agile regulatory structure, and appropriate regulation principles, including FATF Recommendation 10, should be updated with an increased due diligence procedure and a more versatile risk assessment system. This is critical because artificial intelligence will be the biggest technology in fighting financial crime and this will result in an equal development of compliance structures so as to fight money laundering schemes which keep on being developed. Therefore, further studies are to be conducted in the longitudinal study of the usefulness of AI-based AML tools, and further development of interdisciplinary research should be encouraged to gain a clearer insight into the interaction between AI and AML, as well as ethical factors.

References

1. F. P. Patti, "Towards a Global Anti-Money Laundering Law for Crypto-Assets," *SSRN Electronic Journal*, Jan. 2025, doi: 10.2139/ssrn.5949395.
2. R. Anggriawan and M. E. Susila, "Cryptocurrency and its Nexus with Money Laundering and Terrorism Financing within the Framework of FATF Recommendations," *Novum Jus*, vol. 18, no. 2, p. 249, Sep. 2024, doi: 10.14718/novumjus.2024.18.2.10.
3. F. E. A. Longa, "Cryptocurrency and Money Laundering," *American Journal of Industrial*

and Business Management , vol. 15, no. 2, p. 362, Jan. 2025, doi: 10.4236/ajibm.2025.152017.

4. M. G. K. Hemdani, "Cryptocurrencies and the Dark Web: A Gateway to Money Laundering," in *Studies in computational intelligence* , Springer Nature, 2025, p. 217. doi: 10.1007/978-3-031-80557-8_10.

5. M. A. Azero, S. N. A. K. Abdullah, Z. Zakaria, H. Haris, and Y. H. Yusoff, "The Nexus of Cybercrime and Money Laundering: A Conceptual Paper," *Accounting and Finance Research* , vol. 13, no. 2, p. 167, May 2024, doi: 10.5430/afr.v13n2p167.

6. O. S. Igonor, M. B. Amin, and S. K. Garg†, "The Application of Blockchain Technology in the Field of Digital Forensics: A Literature Review," *Blockchains* , vol. 3, no. 1. Multidisciplinary Digital Publishing Institute, p. 5, Feb. 25, 2025. doi: 10.3390/blockchains3010005.

7. H. Yuan, "Governance of Illegal Fundraising Crimes in the Era of Blockchain: A Focus on Characteristics of New Illicit Fundraising," in *Advances in economics, business and management research/Advances in Economics, Business and Management Research* , Atlantis Press, 2023, p. 171. doi: 10.2991/978-94-6463-298-9_19.

8. S. Abdullaeva, "FATF STANDARDS AND THE IMPLEMENTATION OF THE TRAVEL RULE IN PREVENTING CRYPTO-RELATED MONEY LAUNDERING," *YANGI DAVR ILM-FANI INSON UCHUN INNOVATSION G'OYA VA YECHIMLAR* , vol. 1, no. 10, p. 17, Nov. 2025, doi: 10.47390/ydif-y2025v1i10/n04.

9. A. Chetry and U. Sharma, "Anonymity in decentralized apps: Study of implications for cybercrime investigations," *International Journal of experimental research and review* , vol. 32, p. 195, Aug. 2023, doi: 10.52756/ijerr.2023.v32.017.

10. S. A. Raza, M. Shaikh, and K. Tahira, "Cryptocurrency Investigations in Digital Forensics: Contemporary Challenges and Methodological Advances," *Information Dynamics and Applications* , vol. 2, no. 3, p. 126, Sep. 2023, doi: 10.56578/ida020302.

11. S. Subbagari, "Counter Measures to Combat Money Laundering in the New Digital Age," *Digital Threats Research and Practice* , vol. 5, no. 2, p. 1, Oct. 2023, doi: 10.1145/3626826.

12. W. Ahmed, M. M. Alam, M. A. Soomro, and M. R. C. Verginio, "Strengthening the Role of Financial Intelligence Units (FIUs) in Detecting and Preventing Complex Money Laundering Schemes," *Inverge Journal of Social Sciences* , vol. 4, no. 3, p. 298, Sep. 2025, doi: 10.63544/ijss.v4i3.168.

13. A. O. Japinye, "Integrating Machine Learning in Anti-Money Laundering through Crypto: A Comprehensive Performance Review," *European Journal of Accounting Auditing and Finance Research* , vol. 12, no. 4, p. 54, Mar. 2024, doi: 10.37745/ejaafr.2013/vol12n45480.

14. N. Chuanhao, L. Yunbo, and W. Chao, "AI Application in Anti-Money Laundering for Sustainable and Transparent Financial Systems," *arXiv (Cornell University)* , Dec. 2025, doi: 10.48550/arxiv.2512.06240.