Challenges of Law Enforcement in Combating Cryptocurrency Based Money Laundering In Indonesia

Gregorius Widiartana

Faculty of Law, Universitas Atma Jaya Yogyakarta, Indonesia
* Corresponding Author:
Email: g.widiartana@uajy.ac.id.

Abstract.

The rapid development of cryptocurrency as a digital financial asset has introduced new challenges for the prevention and eradication of money laundering crimes. While cryptocurrencies offer efficiency, decentralization, and borderless transactions, these very characteristics also create significant vulnerabilities for misuse, particularly in facilitating illicit financial flows. In Indonesia, the existing legal framework on anti-money laundering, primarily regulated under Law Number 8 of 2010, was formulated prior to the widespread adoption of cryptocurrency and therefore faces limitations in addressing technology-driven financial crimes. This article examines the challenges of law enforcement in combating cryptocurrency-based money laundering in Indonesia through a normative juridical approach. The study analyzes relevant statutory regulations, institutional authority, and enforcement mechanisms involving agencies such as PPATK, Bappebti, the Financial Services Authority, and law enforcement bodies. The findings indicate that law enforcement faces substantial obstacles, including regulatory fragmentation, jurisdictional complexities, difficulties in tracing blockchain-based transactions, evidentiary constraints, and limited technical capacity among enforcement institutions. Furthermore, the absence of comprehensive regulation concerning decentralized finance and non-custodial digital wallets exacerbates enforcement difficulties. This article argues that without regulatory harmonization, enhanced institutional coordination, and the integration of technological capabilities into law enforcement practices, the Indonesian legal system risks lagging behind the evolving landscape of financial crime. Strengthening adaptive legal frameworks is therefore essential to ensure effective anti-money laundering enforcement in the digital asset era.

Keywords: *Cryptocurrency; law enforcement and money laundering.*

I. INTRODUCTION

The rapid advancement of digital technology has fundamentally transformed the global financial system, particularly through the emergence of cryptocurrency as a new form of digital asset. Cryptocurrencies such as Bitcoin, Ethereum, and other blockchain-based instruments offer innovative mechanisms for value transfer that are decentralized, borderless, and highly efficient [1]. These characteristics have positioned cryptocurrencies as attractive alternatives to conventional financial systems, especially in facilitating fast and low-cost transactions across jurisdictions. However, alongside their legitimate uses, cryptocurrencies also present significant risks, particularly in relation to financial crimes such as money laundering, terrorism financing, and other illicit financial activities.Money laundering remains a serious transnational crime that threatens economic stability, financial integrity, and public trust in legal and financial institutions. Traditionally, money laundering has relied on complex financial schemes involving banks, shell companies, and cross-border transactions [2]. The introduction of cryptocurrency has altered this landscape by providing new methods to obscure the origin, ownership, and movement of illicit funds. Features such as pseudonymity, decentralized networks, and the absence of centralized intermediaries complicate conventional detection and enforcement mechanisms [3]. As a result, law enforcement authorities worldwide face unprecedented challenges in adapting existing anti-money laundering (AML) frameworks to the realities of digital financial technologies.In Indonesia, the issue of cryptocurrency-based money laundering presents a unique legal and institutional challenge.

On one hand, Indonesia has demonstrated a growing acceptance of cryptocurrency as a tradable digital commodity under the supervision of the Commodity Futures Trading Regulatory Agency (Bappebti). On the other hand, the use of cryptocurrency as a means of payment remains prohibited, and its regulatory treatment continues to be fragmented across multiple authorities, including Bank Indonesia, the Financial Services Authority (OJK), and the Financial Transaction Reports and Analysis Center (PPATK) [4] This fragmented regulatory landscape raises fundamental questions regarding legal certainty, institutional coordination, and the effectiveness of law enforcement in addressing cryptocurrency-related financial crimes.The primary legal framework governing money laundering in Indonesia is Law Number 8 of 2010 on the Prevention and Eradication of the Crime of Money Laundering. While this law provides a comprehensive basis for combating money laundering in conventional financial systems, it was enacted before the widespread adoption of cryptocurrency and blockchain technology. Consequently, many of its provisions do not explicitly address the technical and legal complexities posed by digital assets [5]. Although electronic information and transactions are generally recognized under Indonesian law, the absence of specific and integrated regulation concerning cryptocurrency-based laundering creates normative gaps that may hinder effective enforcement.

Law enforcement agencies in Indonesia encounter multiple obstacles in addressing cryptocurrency-based money laundering. These challenges include difficulties in identifying beneficial ownership, tracing blockchain transactions across jurisdictions, determining locus delicti in decentralized systems, and meeting evidentiary standards in criminal proceedings. Moreover, the increasing use of decentralized finance (DeFi), privacy coins, and non-custodial wallets further exacerbates enforcement difficulties by reducing the role of regulated intermediaries that traditionally serve as gatekeepers for AML compliance [6]. These developments challenge the foundational assumptions of existing AML regimes, which are largely built upon centralized financial institutions and reporting obligations.From an institutional perspective, the enforcement of AML laws involving cryptocurrency requires effective coordination among regulatory bodies and law enforcement institutions. PPATK plays a central role in analyzing suspicious financial transactions, while the police and prosecutors are responsible for investigation and prosecution. However, the division of authority over cryptocurrency regulation—treated as a commodity rather than a financial instrument—creates ambiguity regarding supervisory responsibility and enforcement jurisdiction [7]. This ambiguity may weaken the state's capacity to respond promptly and effectively to cryptocurrency-based money laundering cases, particularly those involving cross-border elements.Furthermore, the technical nature of blockchain technology demands specialized expertise and technological infrastructure that may not yet be fully developed within law enforcement institutions. While blockchain is often described as transparent and traceable, in practice, transaction tracing requires advanced analytical tools and international cooperation. Without adequate technical capacity and access to relevant data, law enforcement efforts risk becoming reactive rather than preventive [8].

This situation underscores the need for a legal and institutional framework that is not only normatively sound but also operationally effective in the digital era.Against this backdrop, this article seeks to examine the challenges of law enforcement in combating cryptocurrency-based money laundering in Indonesia from a normative juridical perspective. The analysis focuses on evaluating the adequacy of existing legal norms, institutional arrangements, and enforcement mechanisms in responding to the evolving nature of financial crime. Rather than merely describing regulatory developments, this study critically assesses the extent to which Indonesian law has adapted—or failed to adapt—to technological transformation in the financial sector.This research is significant for several reasons. First, it contributes to the growing body of legal scholarship on the intersection between financial technology and criminal law, particularly in the context of developing legal systems. Second, it highlights the practical implications of regulatory fragmentation and technological disparity for law enforcement effectiveness. Third, it offers a normative foundation for future legal reform by identifying key structural and doctrinal challenges that must be addressed to strengthen Indonesia's anti-money laundering regime.Ultimately, the effectiveness of law enforcement against cryptocurrency-based money laundering depends not only on the existence of legal norms but also on the state's ability to integrate legal certainty, institutional coordination, and technological capability. Without a responsive and adaptive legal framework, the rapid evolution of cryptocurrency risks outpacing the law, thereby undermining the broader objectives of financial integrity and public interest protection. This article argues that addressing these challenges is essential to ensure that the Indonesian legal system remains capable of safeguarding economic order and combating sophisticated financial crimes in the digital age.

II. METHODS

This study employs a normative juridical research method aimed at analyzing the legal framework and law enforcement challenges related to cryptocurrency-based money laundering in Indonesia. Normative legal research is appropriate for this study because it focuses on examining legal norms, principles, and doctrines governing anti-money laundering (AML) enforcement, particularly in response to technological developments in digital assets and blockchain systems. Rather than relying on empirical data, this research emphasizes the evaluation of written laws, regulations, and authoritative legal sources to assess their adequacy in addressing emerging financial crimes.The research adopts several complementary approaches. First, a statutory approach is used to analyze relevant Indonesian legislation, including Law Number 8 of 2010 on the Prevention and Eradication of the Crime of Money Laundering, regulations issued by the Commodity Futures Trading Regulatory Agency (Bappebti) concerning crypto asset trading, as well as related policies from Bank Indonesia, the Financial Services Authority (OJK), and the Financial Transaction Reports and Analysis Center (PPATK). This approach enables the identification of normative gaps, overlaps, and ambiguities within the existing regulatory framework, particularly regarding the classification and supervision of cryptocurrency.Second, a conceptual approach is employed to examine key legal concepts such as money laundering, beneficial ownership, locus delicti, and evidentiary standards in the context of decentralized and borderless blockchain systems.

This approach draws upon legal doctrines, scholarly opinions, and international standards, including guidance issued by the Financial Action Task Force (FATF), to assess whether traditional AML concepts remain applicable or require reinterpretation in the digital asset environment.Third, a comparative perspective is selectively applied to contextualize Indonesia’s regulatory approach within broader international developments. While the primary focus remains on Indonesian law, selected references to international practices and standards are used to highlight discrepancies between domestic regulation and globally accepted AML frameworks for virtual assets. This comparative element supports normative evaluation without shifting the research into a fully comparative law study.The legal materials used in this research consist of primary, secondary, and tertiary legal sources. Primary legal materials include statutes, government regulations, and official policy documents. Secondary legal materials comprise peer-reviewed journal articles, books, legal commentaries, and international reports relevant to cryptocurrency regulation and AML enforcement. Tertiary materials, such as legal dictionaries and encyclopedias, are used to clarify technical and conceptual terminology.The analysis is conducted using a qualitative descriptive-analytical method, whereby legal norms are systematically interpreted and critically assessed in light of technological developments and enforcement realities. The results of the analysis are presented in a prescriptive manner, offering normative insights and recommendations aimed at strengthening the effectiveness of AML law enforcement against cryptocurrency-based money laundering in Indonesia.

III. RESULT AND DISCUSSION

Regulatory Fragmentation and Normative Gaps in Addressing Cryptocurrency-Based Money Laundering

The regulation of cryptocurrency in Indonesia reflects a complex and fragmented legal landscape that poses significant challenges to the effective enforcement of anti-money laundering (AML) laws. This fragmentation arises primarily from the absence of a unified legal framework that comprehensively governs cryptocurrency as both a technological and financial phenomenon. Instead, regulatory authority is divided among multiple institutions, each operating within sectoral mandates that were not originally designed to address decentralized digital assets. As a result, normative gaps and overlaps emerge, weakening the state’s capacity to prevent and combat cryptocurrency-based money laundering.At the core of Indonesia’s AML regime is Law Number 8 of 2010 on the Prevention and Eradication of the Crime of Money Laundering. This law establishes a broad framework for identifying, tracing, and confiscating proceeds of crime, as well as defining the roles of reporting entities and law enforcement institutions. However, the law was enacted in a period when cryptocurrency and blockchain technology had not yet become integral to the global financial system [9]. Consequently, the statutory provisions are largely premised on conventional financial intermediaries such as banks and other regulated financial institutions. The absence of explicit references to virtual assets, digital wallets, or blockchain-based transactions creates interpretive uncertainty when applying the law to cryptocurrency-related cases.This uncertainty is compounded by the legal classification of cryptocurrency in Indonesia.

Cryptocurrency is recognized as a tradable digital commodity under the supervision of the Commodity Futures Trading Regulatory Agency (Bappebti), rather than as a financial instrument subject to comprehensive financial regulation [10]. While this approach provides legal certainty for crypto asset trading, it simultaneously limits the scope of financial supervision traditionally associated with AML compliance. Commodity-based regulation focuses primarily on market conduct and consumer protection, rather than on systemic financial integrity and illicit financial flows. As a result, AML obligations imposed on crypto asset service providers may be less robust than those applied to financial institutions under the supervision of the Financial Services Authority (OJK).The fragmentation of regulatory authority further exacerbates normative gaps. Bank Indonesia maintains authority over payment systems and prohibits the use of cryptocurrency as a means of payment, while OJK oversees financial services institutions, and PPATK functions as the central financial intelligence unit responsible for analyzing suspicious transaction reports. Each institution operates within its own regulatory domain, yet cryptocurrency-based money laundering often transcends these boundaries [11]. The lack of a clearly defined lead authority for AML supervision of cryptocurrency activities creates ambiguity regarding accountability, coordination, and enforcement priorities. This institutional fragmentation undermines legal certainty and weakens the coherence of the AML framework.Normative gaps are also evident in the regulation of emerging cryptocurrency ecosystems, particularly decentralized finance (DeFi), non-custodial wallets, and peer-to-peer transactions.

Existing Indonesian regulations largely focus on centralized crypto asset exchanges that can be subjected to licensing and reporting obligations. However, DeFi platforms operate without centralized intermediaries, and non-custodial wallets allow users to retain full control over their digital assets without relying on regulated service providers [12]. These developments challenge the foundational assumptions of AML regulation, which depend on the presence of identifiable intermediaries acting as gatekeepers for customer due diligence and transaction monitoring. The absence of clear legal norms addressing these decentralized structures leaves significant portions of cryptocurrency activity outside the effective reach of AML enforcement.Another critical normative gap concerns the identification of beneficial ownership in cryptocurrency transactions. While Indonesian AML law emphasizes the importance of identifying beneficial owners to prevent the concealment of illicit proceeds, the application of this concept to pseudonymous blockchain addresses remains legally and technically problematic. Without explicit legal standards governing the attribution of digital wallet addresses to natural or legal persons, law enforcement agencies face difficulties in establishing ownership and control over illicit crypto assets. This gap weakens the evidentiary foundation required for investigation, prosecution, and asset recovery in money laundering cases.From a normative perspective, the fragmented and incomplete regulation of cryptocurrency-based money laundering reflects a broader challenge of legal adaptation to technological change.

Law, as a system of norms, often evolves more slowly than technology, resulting in regulatory lag. In the context of cryptocurrency, this lag manifests in outdated legal definitions, sectoral regulatory silos, and the absence of integrated AML standards for virtual assets. Without normative harmonization, regulatory responses risk being reactive, piecemeal, and inconsistent, thereby reducing their effectiveness.The significance of addressing regulatory fragmentation and normative gaps lies in their direct impact on the effectiveness of law enforcement. Clear, coherent, and comprehensive legal norms are essential to guide institutional action, allocate authority, and ensure legal certainty for both regulators and regulated entities. In the absence of such norms, enforcement efforts may be hindered by jurisdictional disputes, interpretive inconsistencies, and procedural vulnerabilities that can be exploited by sophisticated offenders.Therefore, strengthening the legal framework for combating cryptocurrency-based money laundering in Indonesia requires a deliberate effort to harmonize regulations across sectors and institutions. This includes revisiting the legal classification of cryptocurrency, integrating AML standards for virtual assets into the broader financial regulatory framework, and explicitly addressing decentralized technologies within statutory and regulatory instruments. By closing normative gaps and reducing fragmentation, Indonesian law can better align with international AML standards and enhance its capacity to respond effectively to evolving financial crimes in the digital age.

Institutional and Jurisdictional Challenges in Enforcing Anti-Money Laundering Laws

The effectiveness of anti-money laundering (AML) regimes is not determined solely by the adequacy of substantive legal norms, but also by the institutional architecture and jurisdictional coherence through which those norms are enforced. In practice [13]. AML enforcement frequently encounters complex institutional and jurisdictional challenges that undermine the capacity of states to detect, investigate, and recover proceeds of crime, particularly in the context of transnational and technologically driven financial crimes.At the institutional level, fragmentation of authority constitutes a persistent obstacle to effective AML enforcement. AML regimes typically involve multiple agencies with distinct mandates, such as central banks, financial services regulators, law enforcement bodies, prosecutors, and financial intelligence units (FIUs). While such division of labor is intended to enhance specialization, it often results in overlapping competencies, coordination failures, and regulatory gaps. In many jurisdictions, including Indonesia, regulatory authority over financial systems, payment instruments, and emerging financial technologies is dispersed among different institutions, each operating within its own legal framework [14]. This institutional compartmentalization hampers integrated supervision and delays timely responses to suspicious financial activities.Financial intelligence units, which serve as the central nodes for collecting and analyzing suspicious transaction reports, are particularly affected by institutional constraints. Although FIUs play a crucial role in transforming financial data into actionable intelligence, their effectiveness depends on seamless cooperation with law enforcement and prosecutorial agencies.

In practice, however, information sharing is frequently impeded by bureaucratic procedures, data protection concerns, and differing institutional priorities [15]. As a result, financial intelligence may not be translated efficiently into investigations or asset recovery actions, reducing the overall deterrent effect of AML enforcement. Jurisdictional challenges further complicate AML enforcement, especially in cases involving cross-border transactions. Money laundering schemes often exploit differences between national legal systems, regulatory standards, and enforcement capacities. Criminal proceeds can be rapidly transferred across jurisdictions with varying levels of AML compliance, creating safe havens for illicit funds. The territorial nature of criminal jurisdiction means that domestic authorities are often limited in their ability to investigate transactions, freeze assets, or compel cooperation beyond national borders without resorting to formal mechanisms such as mutual legal assistance treaties (MLATs).While international cooperation frameworks exist, they are frequently criticized for being slow, procedurally rigid, and ill-suited to the speed of modern financial transactions. MLAT processes can take months or even years to yield results, by which time assets may have been dissipated, laundered through multiple layers, or converted into difficult-to-trace forms. This temporal mismatch between legal procedures and financial realities significantly weakens the capacity of states to recover illicit assets and disrupt laundering networks.The rise of digital finance and virtual assets intensifies these jurisdictional challenges.

Cryptocurrency transactions are inherently borderless, often involving decentralized platforms and non-custodial wallets that operate without a central intermediary subject to regulatory oversight. Determining the applicable jurisdiction becomes increasingly problematic when transactions are validated by distributed networks spanning multiple countries, and when service providers lack a physical presence or legal domicile. In such contexts, traditional jurisdictional principles based on territoriality or nationality offer limited guidance, leaving enforcement authorities uncertain about which legal regime applies and which institution bears responsibility.Institutional challenges are also evident in the divergent capacities of states to implement AML standards. Even where legal frameworks formally align with international norms, enforcement effectiveness varies considerably due to differences in technical expertise, financial resources, and political will. Developing countries often face structural constraints that limit their ability to conduct complex financial investigations, trace assets across borders, or engage effectively in international cooperation. These asymmetries create enforcement gaps that can be exploited by transnational criminal networks, further entrenching global patterns of illicit financial flows.

Moreover, institutional incentives within domestic legal systems may prioritize punitive outcomes over asset recovery. Law enforcement success is frequently measured by convictions and custodial sentences rather than by the amount of illicit assets confiscated and returned to the public [16]. This offender-oriented enforcement paradigm diverts attention from the economic dimensions of money laundering and weakens the preventive and restorative objectives of AML laws. Without strong institutional emphasis on asset tracing, freezing, and confiscation, AML enforcement risks becoming symbolically punitive rather than substantively effective.Institutional and jurisdictional challenges represent structural impediments to the effective enforcement of anti-money laundering laws. Fragmented institutional mandates, weak inter-agency coordination, jurisdictional limitations, and the transnational nature of modern financial crimes collectively undermine the capacity of states to combat money laundering in a meaningful way. Addressing these challenges requires not only legal reform, but also institutional redesign, enhanced cross-border cooperation, and a strategic shift toward asset-oriented enforcement that prioritizes the recovery of illicit proceeds as a central objective of AML regimes.

Technological Capacity and Evidentiary Barriers in Cryptocurrency-Based Money Laundering Cases

The effectiveness of law enforcement in combating cryptocurrency-based money laundering is closely linked to the technological capacity of enforcement institutions and their ability to meet evidentiary standards in criminal proceedings. Although blockchain technology is often portrayed as transparent and inherently traceable, the practical reality of investigating cryptocurrency-related crimes reveals significant technical and operational challenges [17]. These challenges are particularly pronounced in jurisdictions where law enforcement institutions have not yet fully developed the specialized expertise and technological infrastructure required to address complex digital asset transactions.One of the primary technological barriers lies in the process of blockchain transaction tracing. While public blockchains allow transaction data to be viewed openly, identifying the real-world actors behind cryptographic addresses requires advanced analytical tools and sophisticated forensic techniques. Law enforcement agencies must rely on blockchain analytics software, data clustering methods, and intelligence-based attribution to establish links between digital wallets and suspected offenders [18]. In the absence of such tools or adequate training, blockchain transparency becomes largely theoretical rather than practically useful for criminal investigations.The increasing adoption of privacy-enhancing technologies further complicates transaction tracing. Privacy coins, such as those employing advanced cryptographic techniques to obscure transaction details, significantly limit the visibility of transaction flows. Similarly, the use of mixing services and tumblers disrupts transactional linkages by combining multiple users' funds, thereby frustrating conventional tracing methods [19].

These technologies challenge the foundational assumption that blockchain transactions can always be followed from origin to destination, thereby undermining investigative strategies that rely on transaction transparency.Decentralized finance (DeFi) platforms introduce additional evidentiary complexities. DeFi operates through smart contracts deployed on blockchain networks without centralized control or identifiable operators. As a result, traditional approaches to law enforcement—such as compelling intermediaries to provide customer data or transaction records—are often ineffective. Non-custodial wallets further reduce the availability of third-party data by allowing users to manage their assets independently of regulated service providers. This erosion of intermediary-based oversight significantly weakens the effectiveness of know-your-customer (KYC) and customer due diligence mechanisms that form the backbone of conventional anti-money laundering regimes.From an evidentiary standpoint, cryptocurrency-based money laundering cases raise challenges related to the admissibility and reliability of digital evidence. Criminal proceedings require evidence that meets established standards of legality, relevance, and authenticity. Blockchain data, while digitally recorded and immutable, must still be properly collected, preserved, and presented to satisfy procedural requirements [20].

This process demands technical competence in digital forensics, as well as clear legal guidelines on the handling of electronic evidence. In the absence of standardized procedures and judicial familiarity with blockchain technology, the evidentiary value of cryptocurrency-related data may be contested during trial.Jurisdictional issues further complicate evidentiary processes. Cryptocurrency transactions often involve multiple jurisdictions simultaneously, with blockchain nodes, service providers, and users located in different countries. Obtaining transaction data or user information may therefore require international cooperation through mutual legal assistance mechanisms. Such processes are often time-consuming and may not align with the speed at which digital assets can be transferred or dissipated. Without timely access to cross-border data, law enforcement agencies risk losing critical evidentiary opportunities.The limitations in technological capacity also affect the preventive function of AML enforcement. When law enforcement institutions lack the tools and expertise to proactively monitor cryptocurrency-related risks, enforcement efforts tend to become reactive, focusing on cases after significant harm has occurred (Kethineni & Cao, 2020).

This reactive approach undermines the broader objectives of AML policy, which emphasize early detection, deterrence, and the protection of financial system integrity. Preventive enforcement requires not only legal authority but also continuous investment in technology, training, and inter-agency collaboration.Normatively, the technological and evidentiary barriers in cryptocurrency-based money laundering cases highlight the need for legal frameworks that integrate technical realities into enforcement strategies. Legal norms should not assume technological neutrality but must account for the specific features of blockchain systems and decentralized networks. This includes recognizing the limitations of existing evidentiary doctrines when applied to digital assets and providing clear guidance on the use of blockchain analytics and digital forensic evidence in criminal proceedings.In conclusion, technological capacity and evidentiary challenges represent critical constraints on the effectiveness of law enforcement against cryptocurrency-based money laundering in Indonesia. Without adequate investment in technical infrastructure, specialized expertise, and legal adaptation, law enforcement institutions risk falling behind the evolving methods of financial अपराध in the digital asset ecosystem. Addressing these barriers is therefore essential not only for successful prosecution but also for ensuring that AML enforcement remains credible, preventive, and responsive in the era of blockchain technology.

IV. CONCLUSION

The rise of cryptocurrency has fundamentally transformed the landscape of financial crime, presenting law enforcement institutions with unprecedented challenges in combating money laundering. Despite blockchain’s theoretical transparency, practical tracing is hindered by sophisticated obfuscation tools such as privacy coins, mixers, and tumblers, as well as by the inherently decentralized nature of DeFi platforms and non-custodial wallets. These developments create significant evidentiary gaps, as traditional investigative techniques and legal mechanisms that rely on intermediaries and centralized record-keeping become ineffective.Furthermore, the limited technological capacity and expertise within enforcement agencies exacerbate the problem, forcing responses to be largely reactive rather than preventive. Without advanced analytic tools, continuous monitoring systems, and cross-institutional cooperation, law enforcement remains unable to detect, investigate, and disrupt illicit cryptocurrency flows before substantial harm occurs. Consequently, the existing AML framework, which was designed for conventional financial systems, struggles to address the evolving risks of decentralized digital finance.To restore the effectiveness of AML efforts, it is essential to enhance institutional capabilities through investment in technology, specialized training, and stronger legal instruments that support proactive surveillance and asset recovery. Only through a combination of technical innovation and regulatory adaptation can authorities keep pace with the rapid evolution of cryptocurrency ecosystems and safeguard the integrity of the financial system.

REFERENCES

[1] S. Abdallah-Ou-Moussa, M. Wynn, and O. Kharbouch,“Blockchain, Cryptocurrencies, and Decentralized Finance: A Case Study of Financial Inclusion in Morocco,” *Int. J. Financial Stud.*,vol.13, no.3,art. no. 124, 2025.

[2] J. Ferwerda, “The economics of crime and money laundering: Does anti-money laundering policy reduce crime?” *Review of Law & Economics*, vol. 9, no. 2, pp. 215–242, 2013, doi: 10.1515/rle-2012-0030.

[3] J. Dote-Pardo and M. T. Espinosa-Jaramillo, “Money laundering risks of cryptocurrencies: Towards coordinated regulatory and technological strategies,” ***Latin American Journal of Blockchain and Cryptocurrencies***, vol. 1, art. 100194, 2025, doi:10.1016/j.latcb.2025.100194.

[4] A. B. Fahmi *et al.*, "Crypto Regulation and Anti Money Laundering in Indonesia: A Comparative European Union and Switzerland," ***J. Pembangunan Hukum Indonesia***, vol. 7, no. 3, pp. 514–541, 2025.

[5] M. Arifin and S. Rahardjo, "Legal Challenges of Anti-Money Laundering Regulation in Indonesia in the Era of Cryptocurrency," ***Journal of Financial Crime***, vol. 28, no. 4, pp. 1191–1205, 2021, doi: 10.1108/JFC-01-2021-0014.

[6] M. Möser, K. Soska, and N. Christin, "Investigating cryptocurrency crimes: Challenges and opportunities for law enforcement," *IEEE Security & Privacy*, vol. 18, no. 3, pp. 45–53, May–Jun. 2020, doi: 10.1109/MSEC.2020.2982290.

[7] Financial Action Task Force (FATF), *Virtual Assets and Virtual Asset Service Providers: Guidance for a Risk-Based Approach*, Paris, France, 2021.

[8] D. H. Saputra and F. Kusumah, "Blockchain Forensics and the Evidentiary Challenges of Crypto-Based Corruption in Developing Countries," ***Indonesian Journal of Criminal Law Studies***, vol. 10, no. 2, pp. 615–658, 2025, doi:10.15294/ijcls.v10i2.28795.

[9] N. P. Sari dan T. Prasetyo, "Keterbatasan Undang-Undang TPPU dalam Mengantisipasi Pencucian Uang Berbasis Aset Kripto," ***Jurnal Legislasi Indonesia,*** vol. 19, no. 3, pp. 321–338, 2022.

[10] S. H. Fahira, D. Daimah, dan I. Mu'amar, "Cryptocurrency Regulation in Indonesia: Regulation Review and Potential Risks from a Cyber Law Perspective," *Indonesian Cyber Law Review*, vol. 1, no. 2, 2024, https://doi.org/10.59261/iclr.v1i2.3

[11] A. B. Fahmi, A. Satya, J. Setiyono, B. Wijayantini, dan H. A. Y. Abusaada, "Crypto Regulation and Anti Money Laundering in Indonesia: A Comparative European Union and Switzerland," ***Jurnal Pembangunan Hukum Indonesia***, vol. 7, no. 3, pp. 514–541, 2025, doi: 10.14710/jphi.v7i3.514-541.

[12] P. Schär, "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets," *Federal Reserve Bank of St. Louis Review*, vol. 103, no. 2, pp. 153–174, 2021, doi: 10.20955/r.103.153-174.

[13] A. Anjani and H. Widiastuti, "The Puzzle of Money Laundering: A Literature Review of Regulations and Implications," ***Journal of Accounting and Investment***, vol. 25, no. 3, 2025.

[14] K. Karyono dan E. Isretno Israhadi, "Challenges and Strategies of Law Enforcement in Eradication of Money Laundering in Indonesia," ***Greenation International Journal of Law and Social Sciences***, vol. 3, no. 4, pp. 1496–1505, 2025.

[15] Y. S. A. Fhatnur, "Dynamics and Strategies of Law Enforcement of Money Laundering Offences in Indonesia," ***Indonesian Journal of Law and Economics Review***, vol. 19, no. 2, May 2024, doi: https://doi.org/10.21070/ijler.v19i2.1286.

[16] R. Hasudungan Sianturi, *"Optimizing the Recovery of Corrupt Assets from the Perspective of Economic Rights and Human Security in Indonesia", Khazanah Hukum*, vol. 7, no. 2, 2025, doi:10.15575/kh.v7i2.44974.

[17] Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). *Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies?* The Review of Financial Studies, 32(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015.

[18] Kethineni, S., Cao, Y., & Dodge, C. (2018). *Use of Bitcoin in darknet markets: Examining facilitative factors on Bitcoin-related crimes*. ***American Journal of Criminal Justice***, 43(2), 141–157. https://doi.org/10.1007/s12103-017-9394-6.

[19] Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014). *Deanonymisation of clients in Bitcoin P2P network*. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 15–29. https://doi.org/10.1145/2660267.2660379.

[20] Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2021). *SoK: Decentralized finance (DeFi)*. Proceedings of the 4th ACM Conference on Advances in Financial Technologies, 30–46. https://doi.org/10.1145/3479722.3480994.

[21] Kethineni, S., & Cao, Y. (2020). *The rise in cryptocurrency crimes and the challenges for law enforcement*. International Criminal Justice Review, 30(3), 325–344. https://doi.org/10.1177/1057567719827052.