West Science Law and Human Rights
Vol. 4, No. 02, April 2026, pp. 170~180

Law Enforcement Strategies Against Crypto-Asset Money Laundering: Challenges in Evidence and Cross-Border Cooperation

Dwi Saleha[1], Munawir[2], Djuhrijjani[3], Nizla Rohaya[4], Muhammad Nazir[5]
[1] Universitas Muhammadiyah Jakarta
[2,5] Universitas Islam Kebangsaan Indonesia
[3,4] Universitas Muhammadiyah Tangerang

Article Info

Article history:

Received Apr, 2026
Revised Apr, 2026
Accepted Apr, 2026

Keywords:

Money Laundering
Digital Evidence
Cross-Border Cooperation
Law Enforcement
Normative Legal

ABSTRACT

This study examines law enforcement strategies in addressing cryptocurrency-based money laundering, with particular emphasis on evidentiary challenges and cross-border cooperation using a normative legal approach. The rapid development of digital assets such as Bitcoin has introduced new complexities in financial crime, enabling illicit actors to exploit decentralized systems and pseudonymous transactions. Through doctrinal analysis of legal frameworks, regulations, and international standards, including those established by the Financial Action Task Force, this research identifies key gaps in the current legal system. The findings reveal that the collection and admissibility of digital evidence remain significant obstacles due to difficulties in linking blockchain transactions to identifiable individuals, as well as limitations in technical capacity and legal procedures. Additionally, cross-border cooperation is hindered by regulatory fragmentation, jurisdictional differences, and slow mutual legal assistance mechanisms. Existing law enforcement strategies—while incorporating regulatory, technological, and institutional approaches are often insufficient and lack integration. This study concludes that strengthening international legal harmonization, enhancing digital forensic capabilities, and reforming cross-border cooperation mechanisms are essential to improving enforcement effectiveness. Furthermore, adaptive legal frameworks are needed to balance innovation in cryptocurrency with accountability and oversight. This research contributes to the development of more responsive legal strategies to combat cryptocurrency-based money laundering in an increasingly globalized digital economy.

Corresponding Author:

Name: Dwi Saleha
Institution Address: Universitas Muhammadiyah Jakarta
e-mail: dwisaleha07@gmail.com

1. INTRODUCTION

The rapid advancement of digital technology has transformed the global financial landscape, particularly through the emergence of cryptocurrencies such as Bitcoin and Ethereum. These decentralized digital assets operate on blockchain technology, enabling peer-to-peer transactions without the need for traditional financial intermediaries. While cryptocurrencies offer significant benefits including efficiency,

transparency, and financial inclusion—they have also introduced new risks, particularly in the realm of financial crime. One of the most pressing concerns is the increasing use of cryptocurrencies as instruments for money laundering, allowing illicit actors to obscure the origin of illegally obtained funds and move them across borders with relative ease. The rise of cryptocurrencies has created a duality where their potential to enhance financial inclusion and transaction efficiency is counterbalanced by the facilitation of illicit activities, particularly money laundering. The decentralized and anonymous nature of these assets complicates law enforcement efforts and presents significant challenges to regulatory bodies [1].

Money laundering, traditionally understood as the process of concealing the origins of illicit funds to make them appear legitimate, has evolved alongside technological innovation. The integration of cryptocurrencies into laundering schemes has significantly complicated law enforcement efforts. Unlike conventional banking systems that are subject to stringent regulatory oversight, many cryptocurrency transactions occur in decentralized environments with varying degrees of anonymity. Techniques such as mixing services, privacy coins, and decentralized exchanges enable offenders to disguise transaction trails, thereby challenging the capacity of authorities to trace and identify criminal activities. Consequently, the traditional legal and institutional frameworks for combating money laundering are increasingly inadequate in addressing the complexities posed by digital currencies. Current anti-money laundering (AML) measures often fall short in tackling the decentralized and anonymous nature of cryptocurrency transactions [2], [3]. To address these challenges, the adoption of blockchain analytics and machine learning technologies is essential for improving tracking capabilities and enhancing regulatory compliance [4], [5].

Law enforcement agencies face significant challenges in addressing cryptocurrency-related crimes, particularly in the evidentiary processes surrounding blockchain transactions. The pseudonymous nature of cryptocurrencies complicates the collection, authentication, and admissibility of digital evidence, requiring advanced investigative tools and legal frameworks to link digital wallet addresses to real-world identities [6]. The global and volatile characteristics of cryptocurrency transactions further complicate the preservation of evidence, especially when data is distributed across multiple jurisdictions with varying legal frameworks and enforcement capacities. These complexities emphasize the urgent need for updated legal standards and procedural mechanisms to incorporate digital forms of evidence within criminal justice systems. The lack of clear regulations regarding the legal status of cryptocurrencies and the challenges posed by cross-jurisdictional issues are central to these problems [7].

In addition to evidentiary challenges, cross-border cooperation remains a critical obstacle in combating cryptocurrency-based money laundering. Cryptocurrency transactions are inherently global and often involve multiple jurisdictions with differing legal frameworks and enforcement capacities. While international mechanisms such as those promoted by the Financial Action Task Force (FATF) aim to establish common standards for anti-money laundering (AML) and counter-terrorism financing (CTF), their implementation varies significantly among countries, creating regulatory gaps that criminals can exploit [8]. Existing instruments like mutual legal assistance treaties (MLATs) are often slow and bureaucratic, limiting the ability of authorities to respond swiftly to evolving digital crimes. Strengthening cross-border collaboration and harmonizing regulatory standards is essential to address these challenges effectively [7].

From a normative legal perspective, the rise of cryptocurrency-related money laundering raises crucial questions about the adequacy of existing legal frameworks. There is a growing need to critically assess whether current laws, principles, and institutional structures can provide legal certainty, ensure justice, and maintain effective enforcement in

the digital era. This includes evaluating the role of international legal cooperation, adapting evidentiary standards, and balancing regulatory control with technological innovation. This study aims to analyze law enforcement strategies in addressing cryptocurrency-based money laundering, focusing on evidence-related challenges and cross-border cooperation. Using a normative juridical approach, the research seeks to identify gaps in existing legal frameworks and propose strategic recommendations to enhance their effectiveness. Ultimately, this study aims to contribute to developing a more responsive and coherent legal system capable of addressing the complexities of financial crime in the digital age.

2. LITERATURE REVIEW

2.1 Concept of Money Laundering in the Digital Era

The rise of cryptocurrencies has significantly transformed traditional money laundering practices, with their inherent characteristics of anonymity and decentralization facilitating new laundering techniques that challenge existing regulatory frameworks. This transformation is evident in the stages of cryptocurrency-based money laundering: during placement, criminals convert illicit funds into cryptocurrencies, obscuring their origins; in layering, techniques like mixing services and decentralized finance (DeFi) platforms enable complex transactions that are difficult to trace; and in integration, funds are reintroduced into the economy through various channels, often using privacy coins to enhance anonymity [5], [9]. Regulatory challenges have arisen as traditional financial regulations struggle to keep pace with cryptocurrency technologies, with DeFi platforms lacking mechanisms to freeze suspicious transactions, complicating law enforcement efforts [9], [10]. To address these challenges, international cooperation and innovative technologies, such as blockchain analytics, are crucial for effective monitoring and prevention [9], [11].

2.2 Cryptocurrency and Blockchain Technology

Cryptocurrencies, particularly Bitcoin, utilize blockchain technology to create a decentralized and transparent financial system, but their pseudonymous nature presents significant challenges for law enforcement, as user identities are obscured behind wallet addresses, making it difficult to track illicit activities. This paradox has allowed cryptocurrencies to be exploited in various criminal enterprises, necessitating a nuanced approach to regulation and enforcement. Bitcoin is linked to approximately $72 billion in unlawful activities annually, including drug trafficking, money laundering, and ransomware attacks [6]. Its use in darknet markets is facilitated by its pseudonymity, enabling illegal transactions [6], while the emergence of privacy coins further complicates regulatory oversight by enhancing anonymity beyond what Bitcoin offers [12]. The lack of a cohesive global regulatory framework leads to inconsistent approaches, creating loopholes for illicit actors, and while measures like "Know Your Customer" (KYC) policies are implemented, their effectiveness is debated,

particularly in jurisdictions with lax regulations [12].

2.3 *Legal Frameworks for Anti-Money Laundering (AML)*

The global fight against money laundering, particularly in the context of cryptocurrencies, is guided by the Financial Action Task Force (FATF) standards, which have been expanded to include virtual assets and virtual asset service providers (VASPs). Guidelines such as the "Travel Rule" have been introduced to enhance transparency and accountability. However, the implementation of these standards remains inconsistent across jurisdictions, creating vulnerabilities that illicit actors can exploit. This inconsistency stems from varying national regulatory frameworks and the rapid evolution of financial technologies, which often outpace existing AML measures. The amendment of FATF Recommendation No. 15 and the adoption of an Interpretative Note in 2019 were significant steps towards addressing money laundering risks associated with virtual assets, but effective implementation at the national level is crucial to prevent jurisdiction-shopping by money launderers [13]. The geographic jurisdictional approach of FATF requires VASPs to be licensed or registered in their jurisdiction of operation, yet challenges remain in establishing supervisory control over foreign entities, hindering enforcement [13], [14]. The disparity in regulatory frameworks is evident in countries like the United States, which has robust Know Your Customer (KYC) and AML standards, while China's prohibitions have driven crypto activities underground and Colombia faces regulatory gaps. This regulatory fragmentation underscores the need for harmonized international measures and cooperation to combat money laundering effectively in the digital asset space [2], [15]. Cryptocurrencies offer significant opportunities for financial inclusion and innovation, but their anonymity and decentralization pose legal risks that facilitate illicit activities. Balancing these opportunities with adequate legal frameworks is essential for fostering a secure financial ecosystem [2], [16].

2.4 *Evidentiary Challenges in Cryptocurrency Investigations*

The challenges of gathering and presenting evidence in cryptocurrency-related cases arise from the unique characteristics of blockchain technology, such as its decentralized storage and cryptographic validation. While blockchain data is inherently tamper-resistant, establishing a clear link between digital transactions and identifiable individuals remains a significant challenge. This complexity is further exacerbated by the need for specialized tools and expertise to trace transactions, especially when obfuscation techniques like coin mixing and chain hopping are used. Blockchain's decentralization complicates the identification of responsible parties [17], while its immutability prevents the modification or deletion of fraudulent evidence, though this also ensures the integrity of data [17]. Law enforcement agencies require advanced tools and

methodologies to analyze blockchain data effectively [18], and the use of obfuscation techniques further complicates investigations [18]. Proposed solutions include the need for standardized investigative protocols to improve digital forensic investigations and the integration of advanced technologies, such as machine learning and AI, to help identify patterns and irregularities in blockchain transactions [18].

2.5 Theoretical Perspectives on Law Enforcement and Legal Adaptation

From a theoretical standpoint, the literature draws on various legal and criminological theories to analyze the challenges posed by cryptocurrency-based money laundering. The theory of legal adaptation suggests that legal systems must evolve in response to technological changes to remain effective. In this context, the rise of cryptocurrencies necessitates the development of new legal norms and enforcement strategies to address emerging forms of financial crime. Institutional theory provides additional insights, emphasizing the role of regulatory bodies and law enforcement agencies in shaping the effectiveness of anti-money laundering (AML) frameworks. The interaction between formal regulations, institutional capacity, and technological innovation determines the success of enforcement efforts.

Furthermore, theories of transnational crime highlight the importance of international cooperation and the limitations of state-centric approaches in addressing globalized criminal activities. The existing literature underscores the complexity of combating cryptocurrency-based money laundering and stresses the need for integrated approaches that combine legal, technological, and institutional perspectives. This study builds upon these theoretical and empirical insights to further explore law enforcement strategies within a normative legal framework, focusing on evidentiary challenges and cross-border cooperation.

3. METHODS

3.1 Research Approach

This study employs a normative juridical approach, which focuses on the analysis of legal norms, principles, and doctrines relevant to cryptocurrency-based money laundering. The normative approach is used to examine how existing legal frameworks regulate the use of digital assets in financial transactions and how these frameworks respond to emerging challenges in law enforcement. Rather than relying on empirical field data, this research emphasizes doctrinal analysis of laws and legal concepts, aiming to assess their adequacy, consistency, and applicability in addressing complex issues related to evidence and cross-border cooperation.

3.2 Type of Research

The type of research conducted is legal doctrinal research (normative legal research). This method is appropriate because the study seeks to analyze written legal sources and interpret their relevance to contemporary issues in cryptocurrency regulation. The research is descriptive-analytical and prescriptive in nature. It not only describes the current legal conditions governing anti-money laundering (AML) in the context of digital currencies but also analyzes legal gaps and formulates recommendations for improving regulatory and enforcement mechanisms.

3.3 Sources of Legal Materials

This study utilizes three categories of legal materials: primary, secondary, and tertiary. Primary legal materials consist of binding legal instruments, including national legislation, international conventions, and regulatory frameworks related to anti-money laundering (AML) and digital financial systems. These include laws governing financial crimes, electronic transactions, and international cooperation mechanisms, along with international standards issued by the Financial Action Task Force, which serve as key references in shaping global AML policies. Secondary legal materials include scholarly literature such as books, journal articles, research reports, and expert opinions that discuss cryptocurrency, blockchain technology, and money laundering, providing theoretical foundations and analytical perspectives that support the interpretation of primary legal sources. Tertiary legal materials consist of supporting references like legal dictionaries, encyclopedias, and other explanatory sources that assist in clarifying legal terminology and concepts used in the study.

3.4 Techniques of Legal Material Collection

The collection of legal materials is conducted through library research (literature study), which involves systematically identifying, gathering, and reviewing relevant legal documents and academic sources. This process includes inventorying applicable laws and regulations related to anti-money laundering and cryptocurrency, examining international legal instruments and policy guidelines, reviewing academic literature and prior research findings, and analyzing legal doctrines and theoretical frameworks. This method ensures that the study is grounded in credible and authoritative sources, enabling a comprehensive understanding of the legal issues under investigation.

3.5 Analytical Method

The analysis of legal materials is carried out using a qualitative approach, incorporating three main techniques. The first is descriptive analysis, which involves describing the existing legal framework governing cryptocurrency and money laundering, including both national and international regulations. The second technique is analytical interpretation, where the study examines legal issues related to evidentiary challenges and cross-border enforcement, identifying inconsistencies, overlaps, or gaps within the current legal system. The third technique is prescriptive analysis, focusing on formulating legal recommendations and proposing improvements to enhance the effectiveness of law enforcement strategies. The analysis is guided by relevant legal theories, including theories of legal certainty, justice, institutional effectiveness, and transnational cooperation, which provide a framework for evaluating the strengths and weaknesses of current legal arrangements.

To ensure the validity and reliability of the research, several measures are applied. Source credibility is maintained by selecting legal materials from authoritative and recognized sources, such as official regulations and peer-reviewed publications. Triangulation of legal materials is employed to cross-reference multiple sources, ensuring consistency and accuracy in legal interpretation. Additionally, the consistency of legal reasoning is maintained by conducting the analysis systematically and logically, ensuring coherence between legal arguments and conclusions. Through these methods, the research aims to produce a rigorous and comprehensive legal analysis that contributes to the development of effective strategies in combating cryptocurrency-based money laundering.

4. RESULTS AND DISCUSSION

4.1 Evolution of Cryptocurrency-Based Money Laundering Practices

The findings of this study indicate that cryptocurrency has significantly

transformed the landscape of money laundering. Unlike traditional laundering methods that rely heavily on financial institutions, cryptocurrency enables direct peer-to-peer transactions without intermediaries, altering the classical stages of money laundering placement, layering, and integration—into more technologically complex processes. In the placement stage, illicit funds are often converted into cryptocurrencies through exchanges or peer-to-peer platforms, capitalizing on the anonymity and pseudonymity of these transactions [19]. The lack of third-party oversight in peer-to-peer networks facilitates this conversion, allowing criminals to obscure the origins of their funds [20]. In the layering stage, sophisticated methods such as coin mixing, chain hopping, and the use of decentralized finance (DeFi) platforms are employed to further obscure transaction trails [21]. Finally, in the integration stage, laundered assets are reintroduced into the legitimate economy through crypto-to-fiat conversions, investments, or digital asset trading, often involving high liquidity assets like real estate or luxury goods [15].

The laundering of illicit funds through cryptocurrencies in Indonesia involves a structured process comprising placement, layering, and integration stages. Each stage utilizes advanced techniques that exploit the unique characteristics of cryptocurrencies, making detection challenging for law enforcement. The regulatory framework in Indonesia, while present, struggles to keep pace with these evolving methods, necessitating updates to laws and enhanced monitoring capabilities [19]. The integration of cryptocurrencies like Bitcoin has become prevalent due to its liquidity and widespread acceptance. However, more sophisticated actors are shifting toward privacy-enhancing cryptocurrencies and decentralized platforms, which further obscure transaction trails. These developments demonstrate that cryptocurrency-based laundering is not only evolving rapidly but also becoming increasingly difficult to detect using conventional enforcement mechanisms.

The complexities involved in cryptocurrency-based money laundering necessitate a reevaluation of existing legal and regulatory frameworks. As cryptocurrencies continue to evolve, the methods used by criminals to launder funds are becoming more sophisticated and harder to trace. The rise of privacy-focused cryptocurrencies and decentralized finance platforms adds another layer of difficulty for regulators, making it clear that the current regulatory measures are insufficient to address the rapidly changing landscape of digital financial crimes. As these trends continue, enhanced monitoring capabilities and updates to legal structures will be crucial in combating the rise of cryptocurrency-based money laundering effectively.

4.2 Legal Challenges in the Collection and Admissibility of Evidence

One of the central findings of this study is the significant difficulty faced by law enforcement in gathering and presenting digital evidence related to cryptocurrency transactions. Although blockchain technology provides a transparent record of transactions, the pseudonymous nature of wallet addresses complicates the identification of perpetrators. Establishing a legal connection between a digital wallet and a specific individual remains a major evidentiary challenge. In many jurisdictions, the admissibility of digital evidence requires strict compliance with procedural rules, including the integrity, authenticity, and chain of custody of the evidence. Cryptocurrency transactions, stored across distributed networks, pose unique challenges in meeting these requirements, as obtaining transaction data may involve accessing information from multiple nodes or service providers located in different countries, raising jurisdictional and legal concerns.

The admissibility of digital evidence, particularly in the context of cryptocurrency transactions, presents significant challenges due to the decentralized nature of blockchain technology and the complexities of legal frameworks. In jurisdictions like Indonesia,

the lack of clear regulations regarding the legal status of cryptocurrencies complicates the integrity, authenticity, and chain of custody requirements essential for evidence admissibility. This situation necessitates advanced forensic methodologies and international cooperation to effectively address these challenges. Cryptocurrencies are often used in illegal activities, which makes it difficult to seize and identify the owners [7]. The absence of clear regulations creates hurdles for law enforcement in handling cryptocurrency evidence, which impacts its admissibility in court [7].

Traditional digital forensic practices are inadequate for investigating decentralized technologies like cryptocurrencies [18]. Advanced tools, including machine learning and blockchain analytics, are essential for reconstructing transaction histories and identifying patterns [18]. Indonesia's dual regulatory stance complicates the treatment of cryptocurrencies as evidence, leading to legal ambiguities [22]. The Criminal Procedure Code does not adequately address the unique characteristics of digital assets, resulting in procedural inefficiencies [22]. Furthermore, obfuscation techniques such as tumblers and privacy protocols significantly reduce the traceability of transactions, necessitating advanced digital forensic tools and blockchain analytics to reconstruct transaction histories. However, the availability of such tools and expertise varies across jurisdictions, creating disparities in enforcement capabilities. From a normative legal perspective, these findings suggest that existing evidentiary frameworks are not fully equipped to address the complexities of digital financial crimes, highlighting the need for clearer legal standards regarding the admissibility of blockchain-based evidence and enhanced technical capacity within law enforcement institutions.

4.3 Limitations of Cross-Border Cooperation Mechanisms

The study reveals that cross-border cooperation remains one of the most significant obstacles in combating cryptocurrency-based money laundering. Cryptocurrency transactions are inherently transnational, often involving multiple jurisdictions within a single transaction chain. Effective enforcement, therefore, requires coordinated action among various national authorities. While international frameworks, such as those developed by the Financial Action Task Force (FATF), provide important guidelines for anti-money laundering (AML) efforts, the implementation of these standards varies significantly across countries. Differences in legal systems, regulatory approaches, and enforcement priorities create gaps that criminals can exploit. In Indonesia, while progress has been made in aligning policies with FATF recommendations, challenges persist due to these differences, particularly in sectors like digital finance and real estate.

Indonesia has undertaken significant policy reforms to align with FATF standards, including strengthening beneficial ownership regulations and expanding supervision over non-financial sectors [23]. Despite these efforts, further harmonization of Indonesia's legal framework with FATF recommendations is necessary to enhance the effectiveness of AML measures [24]. Technological gaps and a lack of skilled human resources hinder the enforcement of AML policies, especially in addressing digital money laundering [25]. The real estate sector presents unique challenges, as the current AML framework may not adequately cover its dynamics, particularly the involvement of construction companies and informal financial operators [26], [27].

Mutual legal assistance treaties (MLATs), which facilitate cross-border investigations, are often criticized for being slow and bureaucratic, and these delays can significantly hinder cryptocurrency-related investigations, where transactions occur in seconds. Issues related to data privacy and sovereignty further complicate the exchange of information between jurisdictions. The findings highlight the need for more agile and efficient mechanisms for international cooperation, including the development of real-time information-sharing systems, the harmonization of legal standards, and the

strengthening of institutional collaboration among law enforcement agencies to tackle the complexities of digital money laundering effectively.

4.4 Evaluation of Current Law Enforcement Strategies

Current law enforcement strategies for combating cryptocurrency-based money laundering encompass regulatory, technological, and institutional approaches, each aiming to address the unique challenges posed by the decentralized and pseudonymous nature of cryptocurrencies. Regulatory strategies focus on implementing Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) laws for Virtual Asset Service Providers (VASPs), including exchanges and wallet providers. Countries like the United States enforce stringent Know Your Customer (KYC) standards, while others, such as Colombia, face regulatory gaps [2]. Harmonizing regulations across jurisdictions is also essential to mitigate risks, with the Financial Action Task Force (FATF) offering guidance to promote consistency in enforcement [28].

Technological strategies involve the use of blockchain analytics and digital forensic tools to trace transactions and identify illicit activities. Advanced tools, including blockchain analysis and artificial intelligence, enhance the ability to monitor suspicious transactions in real time, while digital forensic tools help de-anonymize transactions, making cryptocurrencies less attractive for money [29], [30]. These technologies are vital in addressing the complexities of cryptocurrency-related crimes, but their effectiveness is often constrained by the availability of resources and expertise across jurisdictions.

Institutional strategies emphasize the importance of collaboration among national and international law enforcement agencies. Initiatives like the Joint Chiefs of Global Tax Enforcement (J5) highlight the success of cross-border cooperation in tackling cryptocurrency-related crimes [28]. Despite these efforts, the study finds that these strategies are insufficient in addressing the full scope of the problem. Regulatory frameworks remain fragmented and lag behind technological developments, and the integration among regulatory, technological, and institutional approaches is often lacking, resulting in inefficiencies and gaps in enforcement. As a result, while these strategies have contributed to improving enforcement capabilities, the overall effectiveness remains reduced due to inconsistent legal frameworks and procedural barriers.

4.5 Normative Analysis and Proposed Legal Strategies

Based on the findings, this study proposes several normative legal strategies to enhance the effectiveness of law enforcement in combating cryptocurrency-based money laundering. First, there is a need for greater harmonization of legal frameworks at the international level, which includes adopting uniform standards for regulating cryptocurrencies and virtual asset service providers (VASPs), as well as aligning evidentiary rules across jurisdictions. This would reduce regulatory fragmentation and make enforcement more consistent. Second, legal systems must adapt to accommodate the unique characteristics of digital evidence. Clear guidelines need to be developed for the collection, preservation, and admissibility of blockchain-based evidence, alongside investing in the technical capacity of law enforcement agencies to effectively handle such complex data.

Third, international cooperation mechanisms must be reformed to enable faster and more efficient collaboration across borders. This could involve the establishment of specialized international task forces, the use of digital platforms for real-time information sharing, and simplifying procedures for cross-border investigations. Finally, a balanced regulatory approach is necessary to ensure that anti-money laundering efforts do not stifle innovation in the cryptocurrency sector. Legal frameworks should remain flexible and adaptive, allowing for the integration of new technologies while

maintaining effective oversight and accountability to prevent illicit activities.

5. CONCLUSION

This study demonstrates that cryptocurrency has fundamentally transformed the dynamics of money laundering, creating new challenges for law enforcement in both evidentiary processes and cross-border cooperation. The decentralized and pseudonymous nature of blockchain-based transactions complicates the identification of perpetrators and the collection of admissible digital evidence. Furthermore, the transnational character of cryptocurrency activities exposes significant weaknesses in existing international cooperation mechanisms, which remain fragmented and procedurally inefficient. The study highlights that while cryptocurrency has introduced new risks, current law enforcement strategies have struggled to keep pace with these evolving challenges.

The analysis further shows that current law enforcement strategies—although incorporating regulatory frameworks, technological tools, and institutional collaboration—are not yet fully capable of addressing the complexity of cryptocurrency-related financial crimes. The lack of harmonized legal standards, limited technical expertise, and slow international coordination contribute to enforcement gaps that can be exploited by illicit actors. From a normative legal perspective, it is essential to develop more adaptive and integrated approaches, including harmonizing global regulatory standards, strengthening the legal recognition and handling of digital evidence, and establishing more efficient and technology-driven mechanisms for international cooperation. Additionally, investment in institutional capacity and digital forensic expertise is crucial to enhance enforcement effectiveness. Ultimately, combating cryptocurrency-based money laundering requires a multidimensional strategy that balances legal certainty, technological innovation, and global collaboration, ensuring that legal systems can respond effectively to the challenges of the digital era.

REFERENCES

[1] C. Catalini, "Blockchain technology and cryptocurrencies: Implications for the digital economy, cybersecurity, and government," *Georg. J. Int. Aff.*, vol. 19, pp. 36–42, 2018.

[2] P. A. Cozzo and M. A. Díaz, "Cryptocurrencies and money laundering a comparative analysis of risks and regulations," *J. Law Epistemic Stud.*, vol. 1, no. 1, pp. 24–33, 2023.

[3] M. Tiwari and Y. Zhou, "Understanding the evolving landscape of financial crimes and cybercrimes using cryptocurrencies," in *Innovations in Cryptocrime and Financial Fraud*, IGI Global Scientific Publishing, 2026, pp. 1–30.

[4] A. Sydykova, "CRYPTOCURRENCY TRACKING TECHNOLOGIES: HOW BLOCKCHAIN MONEY LAUNDERING IS BEING COMBATED," *Вестник науки*, vol. 2, no. 5 (86), pp. 736–745, 2025.

[5] H. Verma, "The impact of cryptocurrency on money laundering practices," *African J. Commer. Stud.*, vol. 5, no. 2, pp. 51–60, 2024.

[6] D. Khan, H. Farman, S. Hassan, M. Seelro, and M. H. Mughal, "Cryptocurrency Crimes: A systematic Review on Illicit activities using cryptocurrency (Bitcoin) and challenges for Law Enforcement Agencies," *Pakistan J. Eng. Technol. Sci.*, vol. 12, no. 1, pp. 12–25, 2024.

[7] K. Kartono, N. S. Susanti, S. Soewita, A. Salim, and A. Imron, "Legal Ambiguity in Handling Cryptocurrency Evidence: Challenges and Solutions," *Interdiciplinary J. Hummanity*, vol. 3, no. 11, pp. 768–776, 2024.

[8] S. Dyson, W. J. Buchanan, and L. Bell, "The challenges of investigating cryptocurrencies and blockchain related crime," *arXiv Prepr. arXiv1907.12221*, 2019.

[9] M. Joksimović, M. Paunović, and S. Dedjanski, "MONEY LAUNDERING USING CRYPTOCURRENCIES.," *New Econ. Ekon.*, vol. 18, no. 36, 2024.

[10] C. Albrecht, K. M. Duffin, S. Hawkins, and V. M. Morales Rocha, "The use of cryptocurrencies in the money laundering process," *J. Money Laund. Control*, vol. 22, no. 2, pp. 210–216, 2019.

[11] L. Prendi, D. Borakaj, and K. Prendi, "The new money laundering machine through cryptocurrency: Current and future public governance challenges," *Corp. Law Gov. Rev.*, vol. 5, no. 2, pp. 84–91, 2023.

[12] J. F. Silva and F. de S. Ferreira, "Navigating the Transformative Potential and Legal Challenges of Cryptocurrencies and Blockchain Technology," *Rev. Ft*, pp. 50–51, 2020.
[13] G. Pavlidis, "International regulation of virtual assets under FATF's new standards," *J. Invest. Compliance*, vol. 21, no. 1, pp. 1–8, 2020.
[14] L. De Koker, T. Ocal, and P. Casanovas, "Where's Wally? FATF, virtual asset service providers, and the regulatory jurisdictional challenge," in *Financial technology and the law: Combating financial crime*, Springer, 2022, pp. 151–183.
[15] M. Trifiletti, "Laundering-As-A-Service (Laas): The Emerging Gig Economy of Financial Crime," *J. Econ. Financ. Manag. Stud.*, vol. 0, no. 10, pp. 6736–6746, 2025, doi: 10.47191/jefms/v8.
[16] C. Carucci, *Anti-money laundering in the age of cryptocurrencies*, vol. 10. buch & netz, 2024.
[17] H. F. Atlam, N. Ekuri, M. A. Azad, and H. S. Lallie, "Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions," *Electronics*, vol. 13, no. 17, p. 3568, 2024.
[18] S. A. Raza, M. Shaikh, and K. Tahira, "Cryptocurrency investigations in digital forensics: Contemporary challenges and methodological advances," *Inf. Dyn. Appl*, vol. 2, no. 3, pp. 126–134, 2023.
[19] D. P. Perkasa, "Analisis Hukum Kejahatan Ekonomi Digital Cryptocurrency Sebagai Instrumen Money Laundering di Indonesia," *RIGGS J. Artif. Intell. Digit. Bus.*, vol. 4, no. 2, pp. 5474–5478, 2025.
[20] A. Wardani, M. Ali, and J. Barkhuizen, "Money laundering through cryptocurrency and its arrangements in money laundering act," *Lex Publica*, vol. 9, no. 2, pp. 49–66, 2022.
[21] S. Meighan, "Money Laundering and Crypto-Assets".
[22] I. G. Widhartama, W. Frederik, M. E. Kalalo, and H. Y. A. Bawole, "Confiscation of Crypto Asset Evidence: Legal Challenges in Cybercrime Enforcement in Indonesia," *Int. J. Law, Environ. Nat. Resour.*, vol. 5, no. 2, pp. 157–172, 2025.
[23] N. Mouriska and A. Purwati, "PERAN FINANCIAL ACTION TASK FORCE (FATF) DALAM HARMONISASI PENANGGULANGAN PENCUCIAN UANG GLOBAL," *J. Ris. Multidisiplin Edukasi*, vol. 2, no. 8, pp. 321–334, 2025.
[24] M. A. Soehatman and A. Purwati, "FATF Recommendations dan Implementasi Nasional: Studi atas Efektivitas Harmonisasi Kebijakan Anti-Money Laundering," *J. Ris. Multidisiplin Edukasi*, vol. 2, no. 8, pp. 414–426, 2025.
[25] S. Faizah, L. Marina, and A. Purwati, "Tantangan Implementasi Kebijakan Hukum Internasional terhadap Pencucian Uang Digital di Indonesia," *J. Ris. Multidisiplin Edukasi*, vol. 2, no. 8, pp. 167–176, 2025.
[26] F. Angélico *et al.*, "Real estate anti-money laundering in the Global South–are the laws and policies covering the actors they should cover?," *Trends Organ. Crime*, pp. 1–28, 2025.
[27] S. Ismaeel, "Money Laundering: Impact on Financial Institutions and International Law-A Systematic Literature Review.," *Pakistan J. Criminol.*, vol. 16, no. 4, 2024.
[28] N. S. Uzougbo, C. G. Ikegwu, and A. O. Adewusi, "International enforcement of cryptocurrency laws: Jurisdictional challenges and collaborative solutions," *Magna Sci. Adv. Res. Rev.*, vol. 11, no. 01, pp. 68–83, 2024.
[29] M. B. A. Chamunorwa Chitsungo, "Harnessing Digital Strategies to Combat Cryptocurrency-Enabled Crimes: Addressing Money Laundering, Illicit Trade, and Cyber Threats".
[30] S. Subbagari, "Counter measures to combat money laundering in the new digital age," *Digit. Threat. Res. Pract.*, vol. 5, no. 2, pp. 1–13, 2024.