

Research Horizon

ISSN: 2808-0696 (p), 2807-9531 (e)

Research Horizon

Volume: 05

Issue: 02

Year: 2025

Page: 427-436

Citation:

Aji, K. B., Nugraha, A. S.,

Riyanto, A., Bahri, A. S. &

Mahmutarom. (2025).

Strengthening Indonesia's
Cryptocurrency Regulation
to Combat Money

Laundering: A Comparative

Analysis of Canada and

South Korea's Approaches.

Research Horizon, 5(2), 427-

436.

Strengthening Indonesia's Cryptocurrency Regulation to Combat Money Laundering: A Comparative Analysis of Canada and South Korea's Approaches

Krisna Bramantyo Aji^{1*}, Agung Setya Nugraha¹, Aditiya Riyanto¹, Ahmad Saefuddin Bahri¹, Mahmutarom¹

¹ Universitas Wahid Hasyim, Semarang, Indonesia

* Corresponding author: Krisna Bramantyo Aji (mhsmhunwahas1@gmail.com)

Abstract

This paper explores the challenges posed by cryptocurrency-based money laundering in Indonesia and the need for enhanced legislation to address this growing threat. It highlights the gaps in the current regulatory framework, which lacks specific provisions targeting the unique risks of digital currencies. By comparing the regulatory approaches of Canada and South Korea, the study identifies best practices that Indonesia could adopt to combat cryptocurrency-related crimes. The research emphasizes the importance of implementing targeted legislation for cryptocurrency exchanges, requiring compliance with Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) regulations, and introducing Know-Your-Customer (KYC) procedures and real-name account policies to address the anonymity of digital assets. Furthermore, the paper advocates for strengthening international cooperation, utilizing advanced technologies like blockchain analytics, and increasing public awareness and institutional capacity to effectively tackle cryptocurrency-based money laundering. The findings underscore the need for Indonesia to adopt a more comprehensive and technologically forward-thinking legal framework that aligns with global standards to ensure a safer and more transparent digital financial ecosystem. This research contributes to the ongoing discourse on cryptocurrency regulation and offers recommendations for strengthening Indonesia's efforts in combating illicit financial activities within the digital asset space.

Keywords

Cryptocurrency, Money Laundering, Comparative Legal Analysis, Regulatory Framework, Anti-Money Laundering.

1. Introduction

Technological advancements have consistently reshaped economies, societies, and even criminal activities. Among the most transformative developments in recent years has been the rise of cryptocurrencies. Initially hailed as a revolutionary form of decentralized digital currency, cryptocurrencies like Bitcoin have not only transformed the way people invest and transact but have also presented new challenges for law enforcement and financial institutions (Putri et al., 2023). A particularly concerning issue that has emerged is the use of cryptocurrencies in facilitating money laundering, a crime that continues to undermine financial systems globally. The decentralized nature and relative anonymity of cryptocurrency transactions make it an appealing tool for criminals seeking to disguise illicit financial activities. As cryptocurrencies become more integrated into the global financial ecosystem, their role in money laundering schemes has sparked significant concern, particularly in countries like Indonesia, where there is limited legal infrastructure to combat this issue (Alhakim et al., 2024).

In recent years, cryptocurrencies have grown in popularity and usage, not just as investment assets but also as instruments for criminal activities (Haq et al., 2021; Teichmann & Falker, 2021; Nizovtsev et al., 2022; Chandra et al., 2023). These digital assets operate independently of traditional financial systems, allowing for cross-border transactions that can evade the watchful eyes of regulatory authorities. The anonymity provided by cryptocurrencies makes it particularly challenging for law enforcement to trace and identify illicit funds. This has led to an increase in their use in money laundering, with criminals taking advantage of the anonymity and global reach of digital currencies to move illicitly gained assets without detection. This is not an isolated phenomenon; several countries have witnessed similar trends, with cryptocurrency-based money laundering cases becoming more frequent and more sophisticated (Teichmann & Falker, 2021; Wronka, 2021b; Leuprecht et al., 2023).

The case of money laundering via cryptocurrencies is not just an abstract problem. In Indonesia, for instance, the country's financial intelligence unit, Financial Transaction Reports and Analysis Center (*Pusat Pelaporan dan Analisis Transaksi Keuangan*/PPATK), recently uncovered a money laundering scheme involving cryptocurrencies worth over Rp 800 billion between 2022 and 2024 (Nugroho, 2024). These illicit transactions, often stemming from fraudulent investment schemes, underscore the growing threat that cryptocurrencies pose to national and international financial stability (Putri et al., 2023; Leuprecht et al., 2023). Indonesian authorities have acknowledged the challenges cryptocurrencies present, but the country still lacks a comprehensive legal framework to regulate and prevent their misuse for criminal purposes. As cryptocurrencies continue to gain traction, this regulatory gap becomes increasingly problematic, putting Indonesia's financial security at risk (Wronka, 2022c).

The use of cryptocurrencies for money laundering is exacerbated by existing regulatory and enforcement challenges in Indonesia. While the country recognizes the Rupiah as the only legal tender and has instituted some regulations regarding cryptocurrency transactions, these laws are insufficient to address the complexities of money laundering through digital assets. Cryptocurrency transactions are notoriously difficult to trace, and their international nature complicates enforcement further. This lack of effective oversight creates an environment where criminals can exploit the system with relative ease, thereby increasing the need for robust and forward-thinking regulations to mitigate the risks associated with digital currencies. The issue of cryptocurrency-driven money laundering in Indonesia is not just a matter of regulatory oversight but also a matter of national security. According to Nizovtsev et al. (2022), and Chandra et al. (2023), the ability of criminals to hide

illicit funds in the form of cryptocurrencies not only undermines the integrity of the financial system but also poses a threat to the country's economic stability. The absence of a comprehensive regulatory framework hampers efforts to curb these activities and weakens the enforcement of existing laws. It is clear that Indonesia must act swiftly and decisively to address these issues before they become more entrenched and damaging.

This paper seeks to explore the challenges posed by cryptocurrency-based money laundering in Indonesia and the need for stronger legislation to counteract this emerging threat. By examining the current regulatory landscape and comparing it with international best practices, this study aims to identify key gaps in Indonesia's approach to cryptocurrency regulation. Additionally, the paper will argue that adopting a more comprehensive and technologically forward-thinking legal framework, inspired by successful models from countries like Canada and South Korea, is essential for combating cryptocurrency-related crimes in Indonesia.

2. Literature Review

The rise of cryptocurrencies has introduced new challenges in combating financial crimes, particularly money laundering. The decentralized and pseudonymous nature of digital currencies makes them an attractive tool for criminals seeking to obscure illicit financial flows (Albrecht et al., 2019; Teichmann & Falker, 2021). In Indonesia, the Financial Transaction Reports and Analysis Center (*Pusat Pelaporan dan Analisis Transaksi Keuangan/PPATK*) uncovered cryptocurrency-related money laundering schemes worth over Rp 800 billion between 2022 and 2024, highlighting the severity of the issue (Nugroho, 2024; Limaatmaja, 2024). Despite these risks, Indonesia's regulatory framework remains insufficient to address the complexities of cryptocurrency-based money laundering (Putri et al., 2023; Alhakim & Tantimin, 2024).

A key challenge in regulating cryptocurrency transactions is their inherent anonymity. Unlike traditional banking systems, cryptocurrencies allow users to conduct peer-to-peer transactions without intermediaries, making it difficult for authorities to trace illicit activities (Al-Tawil, 2023; Wang & Hsieh, 2024). Criminals exploit techniques such as "coin mixing" or "tumbling" to further obscure transaction trails, complicating law enforcement efforts (Wegberg et al., 2018; Wardani et al., 2022; Putri et al., 2023). Indonesia's current legal framework lacks specific provisions to counter these methods, leaving regulatory gaps that criminals can exploit (Manthovani, 2023).

Indonesia's regulatory landscape is further complicated by conflicting classifications of cryptocurrencies. While Bank Indonesia prohibits their use as a payment method, the Commodity Futures Trading Regulatory Agency (*Badan Pengawas Perdagangan Berjangka Komoditi/Bappebti*) treats them as tradable commodities (Putri et al., 2023). This inconsistency creates ambiguity in enforcement, particularly concerning Anti-Money Laundering (AML) measures (Adiyatma & Maharani, 2020). Although Bappebti Regulation Number 8 of 2021 imposes a "Travel Rule" requiring transaction reporting for amounts exceeding USD 1,000, enforcement remains inconsistent due to the decentralized nature of cryptocurrency markets (Fadia & Nusantara, 2023).

Comparative studies of international regulatory frameworks, such as those of Canada and South Korea, offer valuable insights for Indonesia. Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) mandates stringent AML compliance for cryptocurrency exchanges, including Know-Your-Customer (KYC) protocols and suspicious transaction reporting (Leuprecht et al., 2023). Similarly, South Korea's Financial Transaction Information Act enforces a real-name account policy, eliminating anonymity in cryptocurrency transactions

(Anggriawan & Susila, 2024). These measures enhance traceability and deter money laundering, serving as potential models for Indonesia (Renda & Caneppele, 2023).

To strengthen its regulatory framework, Indonesia must adopt targeted legislation addressing cryptocurrency-specific risks, enhance international cooperation, and integrate advanced technologies such as blockchain analytics (Fletcher et al., 2021; Ruiz & Angelis, 2022). Additionally, improving law enforcement capabilities and public awareness is crucial to mitigating cryptocurrency-related financial crimes (Haq et al., 2022; Wronka, 2022a). Without comprehensive reforms, Indonesia's financial system remains vulnerable to exploitation by money launderers leveraging digital assets (Chandra et al., 2023; Wori et al., 2023; Nelson et al., 2024).

3. Methods

This study employs a normative legal research method, focusing on library-based materials to examine the regulatory challenges surrounding cryptocurrency-related money laundering. The research adopts two primary approaches: the statutory approach and the comparative approach, which allow for a comprehensive analysis of existing legal frameworks and their effectiveness in addressing financial crimes involving digital assets. The statutory approach involves a detailed examination of anti-money laundering regulations in jurisdictions with well-developed legal frameworks for cryptocurrency oversight. These include legislative instruments that impose strict compliance requirements on cryptocurrency exchanges, such as customer identification procedures, transaction monitoring systems, and mandatory reporting mechanisms for suspicious activities. By analyzing these regulations, the study identifies operational best practices that could be adapted to Indonesia's legal context.

The comparative approach evaluates Indonesia's existing anti-money laundering laws alongside more advanced regulatory systems. This involves assessing Indonesia's primary money laundering legislation in relation to its cryptocurrency regulations to identify regulatory gaps. The comparison reveals areas where Indonesia's legal framework lacks specific provisions to address challenges such as transaction anonymity, decentralized exchange platforms, and cross-border money laundering risks. Unlike more developed regulatory systems, Indonesia currently lacks a comprehensive legal framework that explicitly addresses the unique challenges posed by digital currencies. Given the dynamic nature of the cryptocurrency market and the limited academic attention this issue has received in Indonesia, this research adopts a descriptive-analytical approach. It systematically reviews and synthesizes existing legal documents, scholarly publications, and relevant case studies to provide a comprehensive overview of the current regulatory environment. The analysis focuses on identifying systemic weaknesses and proposing potential improvements to the legal framework.

The study aims to contribute to the broader academic discussion on cryptocurrency regulation by providing a detailed assessment of regulatory mechanisms and their effectiveness in combating financial crimes. By examining different regulatory models, the research seeks to identify transferable best practices that could enhance Indonesia's legal framework. The ultimate objective is to propose recommendations for developing a more robust and adaptive regulatory system capable of addressing emerging challenges in the digital asset space. This methodological approach ensures a thorough examination of both theoretical and practical aspects of cryptocurrency regulation, while maintaining focus on the specific context of Indonesia's legal system and its current challenges in preventing money laundering through digital assets. The research methodology is designed to provide actionable insights for policymakers and contribute to the development of more effective regulatory frameworks in Indonesia's financial sector.

4. Results

4.1. Challenges of Cryptocurrency-Based Money Laundering in Indonesia

Indonesia faces significant challenges in combating money laundering through cryptocurrencies due to their decentralized and pseudonymous nature, which allows peer-to-peer transactions without intermediaries, complicating efforts to track illicit financial activities (Al-Tawil, 2023; Meiryani et al., 2023; Renda & Caneppele, 2023; Hillman, 2023; Hossain, 2023; Thommandru, 2023; Nelson et al., 2024; Anggriawan & Susila, 2024; Wang & Hsieh, 2024). The anonymity of cryptocurrency transactions, where user identities are not directly linked to wallet addresses, makes it difficult to identify money launderers who obscure the origins of illegal funds. Techniques like "Bitcoin Laundry," where coins are mixed to break transaction histories, further hinder tracing efforts (Putri et al., 2023). Indonesia lacks specific regulations targeting such practices, limiting law enforcement's ability to address money laundering effectively.

The current legal framework for cryptocurrencies in Indonesia is underdeveloped and unclear. Bank Indonesia prohibits cryptocurrencies as payment systems, while the Ministry of Trade classifies them as commodities tradable under the Commodity Futures Trading Regulatory Agency (*Badan Pengawas Perdagangan Berjangka Komoditi/Bappebti*). According to Putri et al. (2023), this regulatory divide creates confusion, particularly regarding their misuse in financial crimes. Indonesia's regulations also lag behind international standards, such as those set by the Financial Action Task Force (FATF) and the Asia-Pacific Group (APG), hindering efforts to combat evolving cryptocurrency-related crimes.

Although Bappebti Regulation Number 8 of 2021 implements the "Travel Rule," requiring virtual asset service providers to share transaction information for amounts above USD 1,000, enforcement is inconsistent due to the decentralized nature of cryptocurrency markets (Albrecht et al., 2019; Wronka, 2021b; Teichmann & Falker, 2021; Fadia & Nusantara, 2023). Monitoring and verifying transactions remain challenging, and regulatory gaps allow non-compliance, undermining anti-money laundering efforts.

Law enforcement faces difficulties tracing and confiscating cryptocurrency assets, which exist in virtual wallets and require specialized tools and knowledge to recover (Kurniawan et al., 2023; Bahamazava & Reznik, 2023; Leuprecht et al., 2023). The ease of transferring cryptocurrencies across borders complicates enforcement, necessitating international cooperation, which is currently underdeveloped (Utkina et al., 2023; Skinner, 2023; Ristic, 2023). Indonesia's Money Laundering Law (Law Number 8 of 2010) criminalizes concealing criminal assets, including those from cryptocurrencies, but lacks clear guidelines for handling anonymous wallets or cross-border transfers (Adiyatma & Maharani, 2020; Manthovani, 2023; Alhakim & Tantimin, 2024). Traditional methods are inadequate for addressing the complexities of digital currencies, and the absence of clear legal protocols slows asset confiscation.

Indonesia has implemented foundational regulations, but these are insufficient to combat cryptocurrency-based money laundering effectively. The decentralized and anonymous nature of cryptocurrencies, combined with an evolving legal landscape, poses significant challenges. Strengthening the regulatory framework, addressing enforcement gaps, and aligning with global anti-money laundering standards through international cooperation are critical for tackling this growing threat.

4.2. International Legal Frameworks for Money Laundering through Cryptocurrency

As cryptocurrencies gain popularity, countries like Canada and South Korea have developed robust regulatory frameworks to combat their potential misuse in illicit activities such as money laundering and terrorism financing. By comparing their

approaches, Indonesia can draw valuable lessons to strengthen its own cryptocurrency regulations.

In Canada, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) governs cryptocurrency regulation. It mandates that Money Services Businesses (MSBs), including cryptocurrency exchanges, establish compliance regimes to detect and prevent money laundering and terrorism financing. MSBs must report suspicious transactions to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), conduct thorough customer identity verification, and maintain detailed transaction records to ensure traceability. Non-compliance can result in severe penalties, including fines, criminal charges, or license suspension. However, challenges arise with decentralized exchanges, which may operate outside these regulations, and privacy-enhancing technologies that obscure user identities, potentially undermining enforcement efforts.

South Korea's regulatory framework, primarily the Act on Reporting and Using Specified Financial Transaction Information, is enforced by the Financial Services Commission (FSC) and the Korea Financial Intelligence Unit (KoFIU). A key feature is the real-name account policy, introduced in 2020, which eliminates anonymous transactions by requiring all cryptocurrency transactions to be linked to verified real-name accounts. This enhances traceability and reduces the risk of money laundering. Additionally, exchanges must implement Know-Your-Customer (KYC) and Customer Due Diligence (CDD) measures to verify customer identities. Non-compliance can lead to significant fines, criminal charges, or license revocation. Like Canada, South Korea faces challenges in regulating decentralized platforms and ensuring consistent compliance across the evolving cryptocurrency landscape.

Both countries emphasize traceability, customer identification, and suspicious transaction reporting, but their approaches differ. Canada focuses on comprehensive compliance regimes and record-keeping, while South Korea's real-name policy directly targets anonymity, a key enabler of illicit activities. Both frameworks face difficulties in regulating decentralized exchanges and adapting to new technologies.

Indonesia can learn from these models to develop its own regulatory framework. Adopting Canada's emphasis on compliance regimes and transaction reporting, combined with South Korea's real-name account policy, could help Indonesia enhance transaction traceability and prevent anonymous transactions. Robust KYC and CDD measures would further strengthen efforts to combat cryptocurrency-related crimes. However, Indonesia must also address the challenges of regulating decentralized platforms and keeping pace with technological advancements.

By integrating elements from Canada and South Korea's frameworks, Indonesia can create a balanced and effective regulatory environment. This approach would safeguard against money laundering and terrorism financing while fostering the growth of its cryptocurrency market. A comprehensive framework that ensures transparency, accountability, and adaptability will position Indonesia to address the risks of cryptocurrency misuse while supporting innovation in the digital economy.

4.3. Recommendations for Strengthening Indonesia's Cryptocurrency Regulation

Indonesia faces a surge in cryptocurrency-related money laundering, with suspicious transactions exceeding Rp 800 billion from 2022 to 2024, driven by fraudulent investment schemes exploiting cryptocurrencies' anonymity, as reported by the Financial Transaction Reports and Analysis Center (*Pusat Pelaporan dan Analisis Transaksi Keuangan/PPATK*). To address this, Indonesia can draw on Canada and South Korea's regulatory frameworks to strengthen its approach to combating cryptocurrency-based financial crimes.

Indonesia's current regulations, overseen by Bappebti, treat cryptocurrencies as investment commodities but lack specific provisions targeting money laundering risks. Existing laws like the Money Laundering Law and Criminal Procedure Code

do not adequately address cryptocurrencies' unique traits, such as anonymity and decentralization. To bridge this gap, Indonesia should develop a dedicated legal framework for cryptocurrency exchanges, modeled on Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and South Korea's Act on Reporting and Using Specified Financial Transaction Information. This framework would mandate exchanges to implement robust Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) measures, including Know-Your-Customer (KYC) protocols, transaction monitoring, and reporting suspicious activities to the PPATK. Centralized transaction databases could enhance traceability, even in decentralized networks.

A key challenge is cryptocurrencies' anonymity, which enables criminals to obscure illicit funds. Adopting South Korea's real-name account policy, requiring transactions to be linked to verified identities, would reduce anonymity and hinder money laundering. Extending KYC requirements to cryptocurrency wallet providers could further strengthen transaction traceability. Canada's approach, emphasizing compliance regimes and record-keeping, could also guide Indonesia in ensuring exchanges maintain detailed transaction logs for investigation purposes.

International cooperation is critical due to cryptocurrencies' global nature. Aligning with global standards and collaborating with bodies like Canada's FINTRAC and South Korea's KoFIU would improve cross-border transaction tracking and freezing, particularly for decentralized exchanges (DEX) and coin mixers used to obscure funds. Establishing a centralized monitoring body, similar to FINTRAC, would enhance oversight of cryptocurrency activities. To bolster detection, Indonesia should leverage advanced technologies like blockchain analytics and machine learning to identify suspicious transaction patterns in real-time. These tools can analyze public blockchain data to flag illicit activities, enabling proactive intervention before funds are laundered or moved across borders. Investing in such technologies would strengthen Indonesia's regulatory capabilities.

Public and institutional awareness is another priority. Many Indonesians lack understanding of cryptocurrency risks. Educational campaigns, in partnership with exchanges and financial institutions, can inform the public. Additionally, specialized training for law enforcement on tracking and seizing cryptocurrency assets would enhance enforcement capacity. By adopting a comprehensive legal framework, leveraging technology, fostering international cooperation, and raising awareness, Indonesia can effectively combat cryptocurrency-related money laundering. Drawing on Canada's compliance-focused approach and South Korea's real-name policy, Indonesia can create a transparent and secure digital financial ecosystem, balancing innovation with robust defenses against illicit activities.

5. Discussion

Nugroho (2024), revealed that Indonesia's escalating cryptocurrency-based money laundering, with suspicious transactions surpassing Rp 800 billion from 2022 to 2024, underscores the urgent need for a robust regulatory framework. The decentralized and pseudonymous nature of cryptocurrencies complicates tracking illicit funds, as noted by Al-Tawil (2023), and Putri et al. (2023), who highlight how techniques like "Bitcoin Laundry" obscure transaction histories. Indonesia's regulatory gaps, including the absence of specific laws targeting cryptocurrency misuse, exacerbate these challenges (Adiyatma & Maharani, 2020). Drawing on Canada and South Korea's frameworks, Indonesia can address these issues by enhancing legal clarity, traceability, and enforcement.

Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) mandates stringent compliance for cryptocurrency exchanges, requiring suspicious transaction reporting to FINTRAC and robust KYC measures (Leuprecht et al., 2023). This ensures traceability but struggles with decentralized

exchanges (DEXs), which often evade regulation (Assalmani, 2021; Wronka, 2022a). South Korea's real-name account policy, enforced under the Act on Reporting and Using Specified Financial Transaction Information, eliminates anonymous transactions, significantly reducing money laundering risks (Wang & Hsieh, 2024). However, both nations face challenges in regulating DEXs, a concern echoed in Indonesia's context (Alhakim & Tantimin, 2024).

Indonesia's current framework, where Bappebti regulates cryptocurrencies as commodities, lacks targeted AML/CTF provisions (Putri et al., 2023). The "Travel Rule" under Bappebti Regulation Number 8 of 2021 is a step forward but suffers from inconsistent enforcement due to decentralization (Albrecht et al., 2019). Adopting Canada's compliance-focused approach and South Korea's real-name policy could bridge these gaps. A dedicated legal framework mandating KYC, CDD, and centralized transaction databases would enhance traceability, as suggested by Antwi et al. (2023). Extending KYC to wallet providers, as proposed by Wronka (2022b), could further curb anonymity.

International cooperation is vital given cryptocurrencies' cross-border nature. Aligning with FATF and APG standards, as recommended by Anggriawan and Susila (2024), and collaborating with bodies like FINTRAC and KoFIU would improve cross-border tracking (Utkina et al., 2023). Blockchain analytics and machine learning, as advocated by Ruiz and Angelis (2022), can detect suspicious patterns in real-time, addressing enforcement challenges noted by Kurniawan et al. (2023). Public awareness campaigns and law enforcement training, emphasized by Haq et al. (2022), are critical to building capacity. By integrating Canada's compliance regimes and South Korea's real-name policy, Indonesia can create a transparent digital financial ecosystem. Addressing DEXs and leveraging technology, as suggested by Fletcher et al. (2021), will enhance enforcement. These reforms, rooted in global best practices, will balance innovation with robust AML/CTF measures, ensuring Indonesia effectively combats cryptocurrency-related financial crimes.

6. Conclusion

Indonesia faces critical challenges in combating cryptocurrency-based money laundering, primarily due to the decentralized, anonymous nature of digital currencies. The current regulatory framework is insufficient, lacking clear and specific provisions to address the unique risks posed by cryptocurrencies. Through a comparative analysis of Canada and South Korea's regulatory frameworks, this paper identifies gaps in Indonesia's approach, emphasizing the need for a more robust legal structure. Canada's stringent compliance measures, including customer identification and transaction reporting, and South Korea's real-name account policy offer valuable insights for strengthening Indonesia's regulations. By adopting similar legislation for cryptocurrency exchanges, such as mandatory Know-Your-Customer (KYC) protocols and transaction monitoring, Indonesia could enhance its ability to trace and prevent illicit activities.

Additionally, Indonesia must address the challenges of cross-border transactions and decentralized exchanges by improving international cooperation and utilizing advanced technologies like blockchain analytics. Strengthening public awareness and institutional capacity will also play a pivotal role in combating money laundering. Ultimately, adopting a comprehensive and technologically forward-thinking legal framework, aligned with international anti-money laundering standards, is crucial for creating a safer and more transparent digital financial ecosystem in Indonesia. With concerted efforts from regulators, law enforcement, and financial institutions, Indonesia can effectively mitigate the risks posed by cryptocurrency-related crimes and strengthen its defenses against financial misconduct.

References

- Adiyatma, S. E., & Maharani, D. F. (2020). Cryptocurrency's Control in the Misuse of Money Laundering Acts as an Effort to Maintain the Resilience and Security of the State. *Lex Scientia Law Review*, 4(1), 70-82.
- Albrecht, C., Duffin, K. M., Hawkins, S., & Morales Rocha, V. M. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control*, 22(2), 210-216.
- Alhakim, A., & Tantimin, T. (2024). The Legal Status of Cryptocurrency and Its Implications for Money Laundering in Indonesia. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, 11(2), 231-253.
- Al-Tawil, T. N. E. (2023). Anti-money laundering regulation of cryptocurrency: UAE and global approaches. *Journal of Money Laundering Control*, 26(6), 1150-1164.
- Anggriawan, R., & Susila, E. (2024). Cryptocurrency and its Nexus with Money Laundering and Terrorism Financing within the Framework of FATF Recommendations. *Novum Jus*, 18(2), 250-277.
- Antwi, S., Tetteh, A. B., Armah, P., & Dankwah, E. O. (2023). Anti-money laundering measures and financial sector development: Empirical evidence from Africa. *Cogent Economics & Finance*, 11(1), 2209957.
- Assalmani, M. A. (2021). Corporate criminal liability in Indonesian law concerning fund transfer. *Research Horizon*, 1(6), 229-236.
- Bahamazava, K., & Reznik, S. (2023). The comparative analysis of regulations in the Italian Republic and the Russian Federation against cryptolaundrying techniques. *Journal of Money Laundering Control*, 26(4), 787-805.
- Chandra, T. Y., Hossain, M. B., Nor, M. Z. M., & Taher, M. A. Economic Opportunities of Offshore Banking and Regulatory Responses to Money Laundering Risks: A Comparative Study. *Jurnal Hukum*, 40(2), 153-173.
- Fadia, Y., & Nusantara, M. A. Z. (2023). Strengthening Anti-Money Laundering Framework in Online Banking: Bank Indonesia's Initiatives and Countermeasures. *Jurnal Hukum*, 39(2), 252-269.
- Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering money laundering and terrorist financing: A case for bitcoin regulation. *Research in International Business and Finance*, 56(4) 101387.
- Haq, M. Z., Ayub, Z. A., Yusoff, Z. M., & Khan, M. A. A. (2021). Factors influencing anti-money laundering regulatory approaches towards casinos and cryptocurrencies in Bangladesh. *Journal of Money Laundering Control*, 25(2), 445-454.
- Haq, M. Z., Farzana, K. F., & Md, M. (2022). Could banning virtual assets be a breach of the doctrine of legitimate expectation?. *Journal of Money Laundering Control*, 25(4), 719-729.
- Hillman, H. (2024). Pass or play: Should regulators address the money laundering risks posed by cryptocurrencies themselves or await legislative reform?. *Journal of Business Law*, 4(1), 301-328.
- Hossain, M. B. (2023). Acquiring an awareness of the latest regulatory developments concerning digital assets and anti-money laundering. *Journal of Money Laundering Control*, 26(6), 1261-1268.
- Kurniawan, L. D., Rahmawan, A. D., & Manik, J. D. N. (2023). Kajian Kriminologi Terhadap Penggunaan Mata Uang Kripto Sebagai Media Pencucian Uang. *Jurnal Suara Hukum*, 5(1), 89-101.
- Leuprecht, C., Jenkins, C., & Hamilton, R. (2023). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*, 30(4), 1036-1054.
- Limaatmaja, P. J. (2024). Aspek Pidana Terhadap Transaksi Mata Uang Kripto Yang Berpotensi Sebagai Tempat Pencucian Uang. *Lex Positivis*, 2(4), 511-532.
- Manthovani, R. (2023). A Comparative Analysis of Money Laundering Crimes in Indonesia through Cryptocurrency. *International Journal of Cyber Criminology*, 17(1), 196-210.
- Meiryani, M., Soepriyanto, G., & Audrelia, J. (2023). Effectiveness of regulatory technology implementation in Indonesian banking sector to prevent money laundering and terrorist financing. *Journal of Money Laundering Control*, 26(4), 892-908.

- Nelson, F. M., Prosperiani, M. D., Ramadhan, C. R., & Andini, P. P. (2024). Cracking the code: Investigating the hunt for crypto assets in money laundering cases in Indonesia. *Journal of Indonesian Legal Studies*, 9(1), 89-130.
- Nizovtsev, Y. Y., Parfyo, O. A., Barabash, O. O., Kyrenko, S. G., & Smetanina, N. V. (2022). Mechanisms of money laundering obtained from cybercrime: the legal aspect. *Journal of money laundering control*, 25(2), 297-305.
- Nugroho, R. A. (2024). "PPATK Ungkap Pencucian Uang Lewat Kripto Sebesar Rp 800 Miliar!," CNBC Indonesia, April 19, 2024, 12:20, <https://www.cnbcindonesia.com/news/20240419105454-4-531615/ppatk-ungkap-pencucian-uang-lewat-kripto-sebesar-rp-800-miliar>
- Putri, T., Amiludin, A., Ahmad, D. N., & Hidayatulloh, H. (2023). Inadequate cryptocurrency and money laundering regulations in Indonesia (Comparative law of US and Germany). *Yustisia*, 12(2), 129-152.
- Renda, A., & Caneppele, S. (2023). Compliant or not compliant? The challenges of anti-money laundering regulations in crypto assets: the case of Switzerland. *Journal of Money Laundering Control*, 27(2), 363-382.
- Ristic, P. (2023). Cryptocurrency Money Laundering: A New Challenge for the European Anti-Money Laundering Framework. *ZEuS Zeitschrift für Europarechtliche Studien*, 26(2), 189-218.
- Ruiz, E. P., & Angelis, J. (2022). Combating money laundering with machine learning—applicability of supervised-learning algorithms at cryptocurrency exchanges. *Journal of Money Laundering Control*, 25(4), 766-778.
- Skinner, C. P. (2023). Coins, Cross-Border Payments, and Anti-Money Laundering Law. *Harv. J. on Legis.*, 60(2), 285.
- Teichmann, F. M. J., & Falker, M. C. (2021). Cryptocurrencies and financial crime: solutions from Liechtenstein. *Journal of Money Laundering Control*, 24(4), 775-788.
- Thommandru, A. (2023). Smurfing in electronic banking: A legal investigation of the potential for transnational money laundering. *International Journal of Legal Information*, 51(1), 69-76.
- Utkina, M., Samsin, R., & Pochtovyi, M. (2023). Financial intelligence (monitoring) of the transactions with virtual assets: new legislation and best practices of foreign countries. *Journal of Money Laundering Control*, 26(2), 349-360.
- Wang, H. M., & Hsieh, M. L. (2024). Cryptocurrency is new vogue: a reflection on money laundering prevention. *Security Journal*, 37(1), 25-46.
- Wardani, A., Ali, M., & Barkhuizen, J. (2022). Money Laundering through Cryptocurrency and Its Arrangements in Money Laundering Act. *Lex Publica*, 9(2), 49-66.
- Wegberg, R. V., Oerlemans, J. J., & van Deventer, O. (2018). Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 25(2), 419-435.
- Wori, H., Ginting, G., & Polii, J. (2023). Legal Examination of Performance Oversight by the Papua People's Representative Council in Accordance with Community Aspirations Through the Mandate of the Special Autonomy Law. *Research Horizon*, 3(5), 603-610.
- Wronka, C. (2022a). Cyber-laundering: the change of money laundering in the digital age. *Journal of Money Laundering Control*, 25(2), 330-344.
- Wronka, C. (2022b). Anti-money laundering regimes: A comparison between Germany, Switzerland and the UK with a focus on the crypto business. *Journal of Money Laundering Control*, 25(3), 656-670.
- Wronka, C. (2022c). Money laundering through cryptocurrencies-analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control*, 25(1), 79-94.



Copyright: © 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike 4.0 International License (<https://creativecommons.org/licenses/by-sa/4.0/>).