Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.7. No.10 (2026)
Tema/Edisi : Filsafat, Politik dan Etika Profesi Hukum (Bulan Kesepuluh)
https://jhlg.rewangrencang.com/

INDONESIAN ANTI-MONEY LAUNDERING CRIMINAL POLICY OF CRYPTO TUMBLER (MIXER) ON THE DECENTRALIZED EXCHANGE

POLITIK HUKUM PIDANA ANTI PENCUCIAN UANG INDONESIA TERHADAP *CRYPTO TUMBLER (MIXER)* PADA SISTEM PERTUKARAN ASET KRIPTO TERDESENTRALISASI

Olivia Agatha Kusuma, Huberto Gavra Damanik dan Adela Kara Belinda
Universitas Katolik Parahyangan

Corresponding Author : olivia.agatha@unpar.ac.id

Citation Structure Recommendation :

Kusuma, Olivia Agatha, Huberto Gavra Damanik dan Adela Kara Belinda. *Indonesian Anti-Money Laundering Criminal Policy of Crypto Tumbler (Mixer) on The Decentralized Exchange*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.7. No.10 (2026).

ABSTRACT

Normatively, Crypto Tumblers are not explicitly prohibited under the Anti-Money Laundering Law, the P2SK Law, or OJK regulations, although their use may be associated with money laundering activities. Nevertheless, the automated, decentralized and cross-jurisdictional nature of crypto transactions creates significant criminal procedural challenges under both UU TPPU and KUHAP 2025. Given Crypto Tumblers positive role in protecting financial privacy, blanket criminalization is therefore inappropriate and unrealistic. Accordingly, Indonesia should adopt a graduated prohibition model through clear eligibility criteria, whitelisting by OJK and the classification of transactions involving non-compliant Crypto Tumbler users as suspicious transactions as typically monitored by PPATK.

Keywords: Anti-Money Laundering, Criminal Policy, Crypto Tumbler

ABSTRAK

Secara normatif, Crypto Tumbler pada dasarnya tidak dilarang dalam UU TPPU maupun POJK, tetapi penggunaan Crypto Tumbler itu sendiri berpotensi dikaitkan dengan TPPU. Meskipun demikian, tidak tepat mengkriminalisasi Crypto Tumbler secara total karena karakter transaksi kripto yang otomatis, terdesentralisasi dan lintas yurisdiksi akan menimbulkan hambatan penegakan hukum baik berdasarkan UU TPPU maupun KUHAP 2025, terlebih Crypto Tumbler juga masih dibutuhkan untuk perlindungan privasi finansial. Oleh karenanya, Indonesia perlu menerapkan model larangan bertahap melalui penyusunan kriteria Crypto Tumbler yang diperbolehkan, pembentukan *whitelist* oleh OJK, serta pengklasifikasian transaksi pada Crypto Tumbler yang tidak memenuhi kriteria sebagai transaksi mencurigakan seperti pemantauan oleh PPATK.

Kata Kunci: Anti Pencucian Uang, Crypto Tumbler, Kebijakan Pidana

A. INTRODUCTION

Emerging around 2008, crypto assets has rapidly evolved into a prominent vehicle for passive income generation, with Bitcoin standing as the principal pioneer.[1] As a form of digital financial assets, crypto assets were initially conceived as a form of ideological and structural resistance to centralized financial systems (namely, traditional financial regimes administered and/or overseen by designated authorities, e.g.: governments, banks, or other institutions). Such systems were widely perceived to embody inherent weaknesses, including excessive costs, operational inefficiencies and a lack of transparency, rendering them vulnerable to manipulation as a consequence of centralized control by particular entities.[2] In response, proponents sought to create a financial ecosystem detached from the management or supervision of any single authority while remaining reliable, a system now known as Decentralized Finance (DeFi).[3]

With the independence of digital financial systems from traditional finance, ones are able to mitigate the risk of declining intrinsic crypto assets value during periods of fiat currency instability or crisis.[4] This dynamic has likewise become a contributor factor behind the growing reliance of a significant segment of society on crypto assets as a primary investment/income vehicle.[5] Indonesia, in particular, ranked 7th out of 151 countries in terms of crypto adoption according to the Global Crypto Adoption Index 2024, underscoring the considerable promise and expansion potential of its crypto market.[6]

---

[1] Moritz Platt, et al., *Energy Demand Unawareness and the Popularity of Bitcoin: Evidence from Nigeria*, Oxford Open Energy, Vol.2 (2023).

[2] World Bank Group, *Cryptocurrencies and Blockchain*, World Bank Group, Washington, D.C., 2018.; Muhammad Wildan Ichsandi dan Gunardi Lie, *Politik Hukum Digital Banking di Indonesia the Legal Politics of Digital Banking in Indonesia*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.5, No.10 (2025), p.4.

[3] Rabail Adwani dan V Sudhakar Rao, *Decentralized Finance (DeFi): Reshaping Traditional Banking Systems*, European Economic Letters, Vol.15, No.1 (2025).

[4] Manishaben Jaiswal, *Cryptocurrency: An Era of Digital Currency*, International Journal of Creative Research Thoughts, Vol.8, No.1 (2020), p.62.

[5] Halim Hermanto dan Lolita Fitriyana, *Pengaturan Penyitaan Aset Kripto sebagai Hasil Tindak Pidana Pencucian Uang di Indonesia*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.6, No.7 (2025).

[6] Sekar Febriani, *Indonesia Peringkat ke-7 Dunia untuk Adopsi Kripto, Total Transaksi Sentuh Rp 360 Triliun*, Retrieved from https://www.liputan6.com/crypto/read/6201340/indonesia-

Decentralized digital financial system offers several notable advantages. First, crypto assets may be transferred over the internet through peer-to-peer mechanisms with minimal-to-none reliance on intermediary institutions (third parties), in contrast to centralized financial systems, thus enhancing cost and operational efficiency than conventional investment instruments.[7] Second, crypto assets transactions are characterized by a high degree of transparency owing to their foundation in blockchain technology and smart contracts, which enable transactions to be publicly verifiable, immutable and resistant to manipulation. Third, despite such tranparency at the transactional level, the personal identities underlying crypto wallet ownership can be effectively anonymized or at least pseudonymized.[8] This latter feature, however, constitutes a double-edged sword in the context of anti-money laundering efforts. The capacity for anonymity inherent in crypto assets creates an almost ideal mechanism for illicit actors, particularly at the layering stage, where the primary objective is to obscure and dissociate criminal proceeds from their unlawful origins.[9]

Within the decentralized exchange, market participants may further deploy additional tools designed to anonymize, or substantially enhance the anonymity of, crypto transactions and their transactional origin. The use of such tools is conceptually neither incidental nor arbitrary; rather, they are utilized for the heightened privacy and security they purport to offer.[10] Specifically, these mechanisms are designed to shield crypto transactions from cyber threats, including hacking and de-anonymization techniques, for instance by preventing the disclosure of public keys that operate as pseudonymous addresses concealing the identity of wallet holders.[11] Elevated levels of privacy, therefore, are of particular significance for actors who utilize crypto assets in commercial contexts,

---

peringkat-ke-7-dunia-untuk-adopsi-kripto-total-transaksi-sentuh-rp-360-triliun?page=3#google_vignette, Accessed 19 Desember 2025.

[7] Dimaz Ankaa Wijaya, *Mengenal Bitcoin dan Cryptocurrency*, Puspantara, Medan, 2016.

[8] Manishaben Jaiswal, *Op.Cit.*, p.66.

[9] Dwiki Putra Perkasa, *Analisis Hukum Kejahatan Ekonomi Digital Cryptocurrency sebagai Instrumen Money Laundering di Indonesia*, RIGGS: Journal of Artificial Intelligence and Digital Business, Vol.4, No.2 (2025), p.5476.

[10] Bruno Moslavac, *Cryptocurrency Tumbler: Legality, Legalization, Criminalization*, Revista Acadêmica Escola Superior do Ministério Público do Ceará, Vol.11, No.2 (2019), p.211.

[11] István András Seres, et al., *MixEth: Efficient, Trustless Coin Mixing Service for Ethereum*, Proceding International Conference on Blockchain Economics, Security and Protocols (2019).

as they facilitate the protection of sensitive business information and the preservation of transactional confidentiality.

One of the DeFi tools designed to enhance financial privacy is the Crypto Tumbler, commonly referred to as Crypto Mixers. In essence, a Crypto Tumbler constitutes a tool or service that commingles a user's crypto assets transactions with those of other users through a sequence of artificial or obfuscating transfers, thus rendering the origin and destination of the assets difficult, if not nearly impossible, to trace.[12] Although there have been no reported enforcement cases involving Crypto Tumblers in Indonesia, other jurisdictions have identified their large-scale use for money laundering purposes. Notable examples include Tornado Cash, Bitcoin Fog and Helix, all of which share similarities that Crypto Tumblers were used to launder proceeds of crimes such as drug trafficking, fraud and cybercrime.[13]

Several previous studies have also addressed issues relating to Crypto Tumblers, including: (1) Pascal Tippe and Christoph Deckers, *Unmixing the Mix: Patterns and challenges in Bitcoin mixer investigations*; (2) Pakki J. *et al*., *Everything You Ever Wanted to Know About Bitcoin Mixers (But Were Afraid to Ask);* (3) Nurjaman and Prayuti, *Celah Regulasi Penegakan Hukum Dalam Mengatasi Pencucian Uang Dari Kejahatan Ekonomi Melalui Aset Digital Di Indonesia*; (4) Elaine Chan and Sion Yoong Tian, *Decentralised finance (DeFi): a game-changer or just a passing fad.* Nevertheless, previous studies have primarily examined Crypto Tumblers as instruments of money laundering and the challenges associated with their enforcement, while paying limited attention to their potential legitimate uses. To fill this gap, this research offers a novel perspective by demonstrating that Crypto Tumblers may also provide benefits when used for legitimate purposes, particularly in safeguarding financial privacy within business activities. This variable is important in formulating future criminal policy recommendations for Indonesia, as it enables policymakers to address regulatory gaps in the crypto ecosystem while balancing criminal law concerns with legitimate business interests.

---

[12] Dimaz Ankaa Wijaya, *Op.Cit*., p.6.

[13] United States Attorney's Office District of Columbia, *Operator of 'Bitcoin Fog' Sentenced to More Than 12 Years in Prison for Running Notorious Darknet Cryptocurrency Mixer*, Retrieved from https://www.justice.gov/usao-dc/pr/operator-bitcoin-fog-sentenced-more-12-years-prison-running-notorious-darknet, Accessed 22 Desember 2025.

The problem within Indonesia's current crypto asset legal framework is that, at present, the operation and use of Crypto Tumblers are neither expressly prohibited nor specifically regulated, as the existing legal framework contains no provisions that explicitly govern such practices, including under the P2SK Law (Law No. 4 of 2023) and POJK 27/2024. This situation creates what is commonly referred to as a legal vacuum. Against this regulatory background, it becomes particularly salient to examine the prospective trajectory of Indonesia's criminal policy in addressing Crypto Tumblers, especially given their relatively unrestricted use by participants in the decentralized exchange (DEX).[14] This issue gives rise to a profound regulatory dilemma, situated at the interesection of anti-money laundering imperatives, the legitimate interests of crypto assets users for financial privacy and security, alongside the necessity of preserving regulatory space for the continued development of DeFi technologies without precipitating the risks of overcriminalization.

Therefore, it is crucial to determine whether Indonesia should criminalize Crypto Tumblers within the framework of anti-money laundering policy or instead accord them legal recognition and subject their use solely to economic regulation. This issue, as a matter of course, stems from the legitimate benefits that Crypto Tumblers offer in terms of financial privacy and security, particularly in business-oriented contexts. Drawing upon the foregoing background, this study advances a single central research question: what should be the appropriate orientation of Indonesia's criminal policy on anti-money laundering in relation to the use of Crypto Tumblers (mixers)? This research aims to examine the legal and policy implications arising from the regulation, or absence of regulation, of Crypto Tumblers. It further seeks to provide constructive recommendations for the Government in addressing potential regulatory gaps resulting from the misuse of Crypto Tumblers within the DEX ecosystem.

[14] Criminal Policy in This Context Refers to How the Government Memformulasikan Hukum Pidana, Baik Hukum Pidana Materiil Maupun Formil, Sehingga yang Dipertimbangkan Juga dari Segi Kapasitas Penegakan Hukumnya di Samping Ketentuan Hukum Pidana Materiil Saja. Sandhi Bagus Permana, *Legal Policy Concerning the Supervision by the Financial Services Authority Supervisory Board*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.6, No.10 (2025).

B. RESULT AND DISCUSSION

1. Financial Privacy in Crypto Ecosystem

This section begins by outlining the conceptual and operational framework of Decentralized Finance (DeFi) and the Crypto Tumblers as integral components of the contemporary digital asset ecosystem. A clear understanding of how decentralized Crypto Tumblers function is essential before engaging with the analysis of anti-money laundering criminal policy. By situating DeFi and Crypto Tumblers within their technological and economic context, this section then provides the necessary analytical foundation for assessing whether and to what extent, decentralized Crypto Tumblers should be addressed through criminal policy, regulatory intervention, or alternative non-penal approaches within the anti-money laundering regime.

The DeFi constitutes a financial services paradigm operating within a decentralized ecosystem. The primary objective of DeFi is to establish a financial system that functions independently of conventional financial institutions.[15] Through DeFi, users are able to conduct financial transactions without reliance on intermediary third parties, as transactions are executed directly on a peer-to-peer basis among users.

Transactions carried out within DeFi services are recorded through blockchain mechanisms, thus rendering users' transactional data transparently accessible to the public. Moreover, the operation of DeFi is facilitated by smart contracts (technological instruments designed to automatically execute and finalize transactional obligations once the parties have fulfilled the terms stipulated in the contract).[16] This design ensures that transactions within DeFi are conducted in a secure, transparent, independent and efficient manner.[17]

---

[15] I Gede Wahyu Antara Kurniawan, et al., *The Rise of Decentralized Finance (DeFi): Opportunities for Disruption in Traditional Financial Models*, Journal of Education, Social & Communication Studies, Vol.2, No.2 (2025), p.129.

[16] *Ibid*..

[17] *Ibid*..

DeFi exhibits features that are fundamentally distinct from those of conventional financial services, which may be broadly categorized into four principal characteristics: (1) the absence of intermediary involvement; (2) enhanced accessibility; (3) a non-custodial nature; and (4) open and transparent systems:[18]

1) The characteristic of no intermediary involvement denotes that DeFi transactions are executed entirely through blockchain technology, operated by open-source code and supported by smart contracts that are pre-programmed to facilitate DeFi applications. Consequently, transactions conducted within the DeFi no longer rely on centralized intermediaries, such as banking institutions, to effectuate financial exchanges.
2) The characteristic of greater accessibility signifies that DeFi services are, in principle, universally accessible without formal restrictions, provided that users possess internet connectivity, an account and crypto assets stored in a digital wallet. The advent of DeFi thus renders access to financial services more flexible and removes many of the barriers commonly encountered in conventional finance, such as credit scoring requirements, employment verification, or disclosure of one's bankruptcy history. Instead, users may obtain crypto assets with less legal requirements.
3) The non-custodial characteristic of DeFi distinguishes it from conventional financial services that require users to relinquish control of their assets to centralized institutions. In DeFi, users retain full control over their crypto assets through self-hosted wallets directly connected to DeFi protocols, without centralized intervention. In other words, no third-party exercises custodial authority over a user's digital assets.
4) The characteristic of open and transparent systems reflects the fact that DeFi operates through open-source protocols that are transparent and accessible to the public, allowing ones verify the underlying code.

[18] Elaine Chan and Sion Yoong Tian, *The Rise of Decentralised Finance (DeFi): Opportunities for Disruption in Traditional Financial Models*, LexisNexis, London, 2022, p.39.

This opennes underscores the accountability of DeFi systems, which predominantly rely on public blockchain infrastructures. Public blockchain mechanism functions as distributed ledgers that record financial transactions in a manner that is openly accessible and broadly disseminated to the public. The data recorded in such blockchains are immutable and resistant to alteration, thus reinforcing the accountability and integrity of the system.[19]

These four aspects of DeFi confer a range of advangtages, particularly the characteristic of transactional transparency, which enables every transaction executed through DeFi applications to be publicly verifiable. Such transparency contributes to increased efficiency, enhanced accountability and greated systemic trust, while simultaneously reducing transaction costs and expanding financial inclusion for populations that have traditionally been underserved by conventional financial systems.[20]

However, notwithstanding the benefits associated with its transparent design, DeFi also entails certain disadvantages that may be acutely experienced by its users, especially traders who are actively engaged in DeFi markets and hold substantial volumes of crypto assets. Cross-protocol or cross-chain transactions, for instance, may readily expose patterns of trading strategies, asset ownership and even one's financial position.[21] Blockchain technology, while offering extensive decentralization and the aforementioned advantages, may thus appear paradoxal from a privacy perspective.[22] Intrusions upon privacy may originate not only from other market participants but also from coercive measures undertaken by law enforcement authorities, such as interception or surveillance, which are now legalized under Indonesia's general criminal procedural law, namely Law No. 20 of 2025 on the Criminal Procedure Code (*Kitab Undang-Undang*

---

[19] Harold Nwariaku, et al., *Blockchain Technology as an Enabler of Transparency and Efficiency in Sustainable Supply Chains*, International Journal of Science and Research Archive, Vol.12, No.2 (2024), p.1780.

[20] I Gede Wahyu Antara Kurniawan, et al., *Op.Cit.*.

[21] Lu Lin, Lingyan Han and Liangmin Wang, *A Privacy-Preserving Cross-Chain Cryptocurrency Transfer Scheme Based on Commitment Scheme and Zero-Knowledge Proof*, Computers and Electrical Engineering, Vol.124 (2025), p.1.

[22] Budi Raharjo, *Uang Masa Depan: Blockchain, Bitcoin, Cryptocurrencies*, Yayasan Prima Agus Teknik, Semarang, 2022, p.22.

Hukum Acara Pidana 'KUHAP'). Accordingly, in order to safeguard their assets, traders may resort to Crypto Tumblers as a means of protectiong their identities and obfuscating their transactional trails.

This, of course, is not to suggest that Crypto Tumblers should be legalized wihtout restriction. Their use should remain subject to regulatory oversight, precisely to ensure that individuals may utilize Crypto Tumblers for legitimate purporses without constantly facing the risk of being criminalized under UU TPPU. The UU TPPU (particularly Article 3, 4, 5) should continue to serve as the primary legal instrument for combating money laundering where Crypto Tumblers are employed to conceal or disguise the proceeds of crime. At the same time, the law must provide adequate space for technological development. In practice, many participants in the crypto community utilize Crypto Tumblers for lawful purposes, particularly to protect their financial privacy and enhance the security of their transactions.

Crypto Tumbler itself is only one of several methods by which crypto assets may be rendered anonymous. Various other techniques are acknowledged to achieve differing degrees of anonymity, including pseudonymous addressing, ring signatures, zero-knowledge proofs, commitments and stealth addressing.[23] Among these mechanisms, Crypto Tumblers have gained particular prominence among crypto users due to the high level of privacy they are able to provide. A Crypto Tumbler constitutes a service designed to mix crypto assets with those of other users by dividing them into multiple fragmented units and redistributing them through a series of transactions. The primary objective of this process is to obfuscate the origin and source of the assets, in which significantly impeding their traceability. In order to operate a Crypto Tumbler, users are generally required to undergo three fundamental stages.[24]

---

[23] Nasser Alsalami and Bingsheng Zhang, *SoK: A Systematic Study of Anonymity in Cryptocurrencies*, IEEE Conference on Dependable and Secure Computing (2019), p.2.

[24] Pascal Tippe and Christoph Deckers, *Unmixing the Mix: Patterns and Challenges in Bitcoin Mixer Investigations*, Forensic Science International: Digital Investigation, Vol.52 (2025), p.2.

At the first stage, the user transfers the crypto assets intended for mixing to a designated address (another crypto wallet). Subsequently, at the second stage, the Tumbler randomly mixing the user's crypto assets with those of other Tumbler users within the liquidity pool in order to generate newly reassigned transactional identifiers. Thereafter, the mixed crypto assets are transmitted to the new address previously specified by the user.[25]

Users of such services may utilize two types of Crypto Tumblers, namely centralized and decentralized Tumblers. Centralized Crypto Tumblers operate through a more practical and streamlined process. However, their operation requires reliance on third-party serivce providers to maintain the confidentiality of user data. Where such confidentiality is not adequately guaranteed, user's privacy may be compromised, particularly in the event that the system is breached by unauthorized actors,[26] or even legally by the authorized actors for law enforcement.[27]

By contrast, decentralized Crypto Tumblers employ a more complex operational structure and demand a higher degree of technical proficiency from users. The mixing process in decentralized Tumblers generally requires a longer time to complete than that of their centralized counterparts. Nevertheless, decentralized Tumblers are widely regarded as offering superior security, as they rely exclusively on peer-to-peer protocols to mix crypto assets without the involvement of any centralized third party.[28]

The existence of Crypto Tumblers continues to be regarded as inherently dilemmatic. On the one hand, such services offer significant benefits to their users, particularly traders engaged in DeFi ecosystems, who utilize Tumblers as a mechanism for safeguarding their crypto assets. Given the transparent design of DeFi, users are inherently exposed to risks of data leakage, de-anonymization and security breaches. The deployment of Crypto Tumblers may mitigate these risks by affording an additional layer

---

[25] *Ibid*..

[26] Lei Wu, et al., *Towards Understanding and Demystifying Bitcoin Mixing Services*, *Towards Understanding and Demystifying Bitcoin Mixing Services*, Proceedings of The Web Conference (2021).

[27] Pasal 112, 113, 136 Kitab Undang-Undang Hukum Acara Pidana, Desember 2025.

[28] *Ibid*..

of privacy protection.[29] This is achieved by severing the link between user's transactional records and their identifiable profiles. In this manner, traders employ Crypto Tumblers to shield their assets from hacking attempts and transactional data breaches, as such services typically rely on cryptographic algorithms designed to withstand cyberattacks, thus impeding unauthorized actors from misappropriating crypto assets or extracting sensitive transactional information.[30]

On the other hand, despite of these advantages, the existence of Crypto Tumblers also entails substantial risks and a pronounced potential for misuse. In particular, such services may be exploited by illicit actors as instruments for money laundering, terrorist financing and other forms of criminal activity. As well as the anti-money laundering enforcement, Crypto Tumblers generate novel legal challenges within the contemporary regulatory landscape.

2. Decentralized Finance (DeFi) and Travel Rule

In a global context,[31] exists an independent intergovernmental organization mandated to set international standards for anti-money laundering efforts named the Financial Action Task Force (FATF). FATF has actively and supposedly kept pace with technological developments in the financial sector.[32] In this regard, the FATF has also issued a series of standards and recommendations for states concerning anti-money laundering measures related to virtual assets. Under Recommendation 16 of the FATF Standards, commonly referred to as the "Travel Rule", the FATF requires Virtual Assets Service Providers to implement core compliance obligations, including but not limited to Know Your Customer (KYC) and Know Your Transaction (KYT) principles, which in the Indonesian context

---

[29] Jaswant Pakki, et al., *Everything you Ever Wanted to Know About Bitcoin Mixers (But Were Afraid to Ask)*, Proceedings Financial Cryptography and Data Security: 25th International Conference (FC 2021) .

[30] Daniel Genkin, Dimitrios Papadopoulos and Charalampos, *Privacy in Decentralized Cryptocurrencies*, Communications of the ACM, Vol.61, No.6 (2018), p.81.

[31] Hanna Rosyidah, Bayu Satya Ndharma and Naya Aulia Zulfa, *Inkonsistensi Aturan Pertanggungjawaban Pidana Pencucian Uang oleh Korporasi: Perlukan Reformulasi?*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.2, No.12 (2021), p.3.

[32] FATF, *The Fath is Leading Global Action to Fight Back*, Retrieved from https://www.fatf-gafi.org/en/the-fatf/what-we-do.html, Accessed 26 Desember 2025.

are understood as *prinsip pemantauan dan pengenalan nasabah dan transaksi*.[33]

Such anti-money laundering policy standards have subsequently been incorporated into various national legislative and regulatory instruments. By way of example, Articles 80, 95 and 96 of Financial Service Authority Regulation No. 27 of 2024 on the Implementation of Digital Financial Asset Trading Including Crypto Assets (hereinafter "POJK 27/2024"), expressly regulate the application of Know Your Customer (KYC) and Know Your Transaction (KYT) principles. POJK 27/2024 constitutes an implementing regulation of the higher law, that is Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector (*Undang-Undang Pengembangan dan Penguatan Sektor Keuangan*, "P2SK Law"), which amended several provisions of Law No. 21 of 2011 on the Financial Services Authority (*Undang-Undang Otoritas Jasa Keuangan*, "OJK Law"). These amendments form the legal basis for the transfer of supervisory authority over crypto assets from the Commodity Futures Trading Regulatory Agency (Bappebti) to the Financial Services Authority (OJK).

The enactment of regulations such as POJK 27/2024 represents the State's effort to balancing between the expansion of digital financial asset trading, including crypto assets, the protection of consumers and the enforcement of anti-money laundering obligations in relation to virtual assets. Nevertheless, not all crypto assets movements fall within the regulatory reach. Article 1 no. 11 and Article 2 of POJK 27/2024 explicitly limits its regulatory subjects, inter alia, to OJK-licensed Digital Financial Asset Trading Operators and Custodial Service Providers. This category corresponds to centralized crypto asset trading, commonly referred to as Centralized Exchange (CEX), which operates under the authorization and supervision of a designated regulatory authority.[34]

---

[33] Financial Action Task Force, *Explanatory Note for Revised Recommendation 16 (R.16)*, Financial Action Task Force, Paris, 2025.

[34] Matteo Aquilina, et al., *Decentralised Dealers? Examining Liquidity Provision in Decentralised Exchanges*, Working Paper, Bank for International Settlements, Basel, 2024, p.11.

By contrast, the crypto ecosystem also encompasses forms of crypto asset trading and storage that remain outside OJK supervision and pose significantly greater challenges for monitoring by the Financial Transaction Reports and Analysis Center (PPATK), such as non-custodial privacy wallets and foreign exchanges operating without OJK authorization (e.g. Binance).[35] These latter forms are generally classified as decentralized crypto asset trading, or Decentralized Exchange (DEX).[36]

The policy standards embodied in Travel Rule were fundamentally designed for the CEX, as they impose anti-money laundering obligations upon Virtual Asset Service Providers and other financial institutions.[37] The application of the Travel Rule to the DEX, therefore, presents a complex challenge, given the very nature of "decentralization", which implies the absence of centralized management or supervisory authority. The Travel Rule cannot be transposed wholesale onto DeFi system whose structural characteristics stands in stark contrast to those of CEX. Accordingly, it remains an open question whether the FATF should revise or recalibrate the Travel Rule to address DeFi-specific risks, or conversely, whether the standarization of DeFi falls outside the appropriate scope of FATF regulation.

The strategic direction adopted by the FATF will inevitably exert influence on national legal frameworks. It must be acknowledged that the anti-money laundering policy standards recommended by the FATF predominantly transcend the domain of criminal law and operate largely within the scope of administrative regulation. This, however, does not render them devoid of implications for the domestic (national) criminal law. Consequently, a more specific and consequential question arises as to whether the use of Crypto Tumblers ought to be inherently regarded as unlawful conduct constituting an element of the offence of money laundering,

---

[35] Alia Yofira Karunian, Muhammad Tanziel Aziezi and Seira Tamara Herlambang, *Unraveling the Vulnerabilities of Abuse and Enforcement of Digital Currency Related to Criminal Offenses*, Indonesian Corruption Watch, Jakarta, 2024, p.45.
[36] Matteo Aquilina, et al., *Op.Cit*..
[37] Financial Action Task Force, *Best Practices on Travel Rule Supervision*, Financial Action Task Force, Paris, 2025, p.4.

or, in other words, whether such use should be expressly criminalized. This inquiry is particularly salient given that criminal policy in the sphere of cybercrime must be coherently aligned with criminal procedural law (formal criminal law) and its actors, as well as the non-penal policy instruments, all of which function in a complementary and inseparable manner.[38] Indeed, even though Indonesia already has the UU TPPU and KUHAP 2025, the reality remains that not all jurisdictions are adequately prepared to address the increasingly sophisticated patterns of crime committed digitally.[39] To facilitate this analysis, the following discussion examines the legal position of Crypto Tumblers within the Indonesian legal system.

3. Legality of Crypto Tumbler

At present, the legal status of Crypto Tumblers in Indonesia remains positioned within a grey area. This grey area falls between the absence of the law in books and the presence of the law in action. Normatively, there is no explicit prohibition on the use of Crypto Tumblers; however, this absence of prohibition does not equate to their affirmative legal recognition. Indonesia has far not enacted any statutory provision that explicitly mention or qualify the use of Crypto Tumblers as an unlawful act, nor specifically govern the use of Crypto Tumblers.[40] Accordingly, Crypto Tumblers cannot be said to be prohibited under the existing law in books. In light of the principle of legality *(nullum crimen sine lege)*, this normative vacuum may give rise to the perception that the use of Crypto Tumblers does not constitute a violation of law.[41] Nevertheless, the absence of an explicit prohibition does not automatically entail that Crypto Tumblers possess affirmative legal legitimacy, as perceived within the law in action.

---

[38] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana, Jakarta, 2007, p.238-239.

[39] Alejandro Morion Ruben Thomas and Happy Yulia Anggraeni, *Cybercrime dan Media Sosial: Analisis Hukum terhadap Tren Peningkatan Tindak Pidana di Era Digital*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.6, No.7 (2025), p.4.

[40] Adinda Melinia Sari, Sari Mandiana and Paula Paula, *Analisa Pertanggungjawaban Pidana atas Penggunaan Aset Kripto sebagai Sarana Tindak Pidana Pencucian Uang*, Aliansi: Jurnal Hukum, Pendidikan dan Sosial Humaniora, Vol.1, No.2 (2024).

[41] Randa Risgiantana Ridwan, *Transaksi Mata Uang Virtual (Cryptocurrancy) sebagai Celah Terjadinya Tindak Pidana Pencucian Uang*, Jatiswara: Jurnal Ilmu Hukum, Vol.37, No.3 (2022), p.358.

In contrast, when examined from the perspective of law in action, the use of Crypto Tumblers in practice widely regarded as posing serious challenges to the anti-money laundering efforts. Empirically, crypto asset transactions that have passed through Crypto Tumblers may still be detected and classified by the Financial Transaction Reports and Analysis Center (PPATK) as Suspicious Financial Transactions, rendering them susceptible as money laundering methods. Such detection becomes possible when the flow of funds ultimately enters government-supervised financial systems, notwithstanding the existing limitations in technological infrastructure for comprehensive monitoring and detection.

Financial institutions and law enforcement authorities may encounter substantial difficulties in tracing fund flows that have passed through transaction-mixing mechanisms.[42] Therefore, the use of Crypto Tumblers is generally categorized as a high-risk activity within the framework of anti-money laundering.[43] This classification is logically not premised on the assumption that all users of Crypto Tumblers are criminal actors, but rather on the inherent characteristics of Crypto Tumblers themselves, which create significant opportunities for misuse. Proceeds of crime may be readily "cleansed" through these mechanisms before ultimately re-entering the formal and legitimate financial system.

Crypto Tumblers possess a high potential to be utilized as instruments for money laundering offences (as a criminogenic factor), given their functional capacity to conceal the origin of assets by severing the link between the source of funds and the ultimate recipient through transaction-mixing mechanisms.[44] Accordingly, although Crypto Tumblers are not yet normatively prohibited, they are functionally aligned with established money laundering typologies. They effectively capable of eliminating the audit trail that constitutes a cornerstone of anti-money laundering enforcement.[45]

---

[42] *Ibid.*. ; Tegar San Putra, et al., *Keabsahan Alat Bukti Digital dalam Pembuktian Kasus Phantom Hacker Scam*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.7, No.7 (2026).

[43] Randa Risgiantana Ridwan, *Op.Cit.*.

[44] Dwiki Putra Perkasa, *Op.Cit.*.

[45] *Ibid.*. ; Satria Angga Kurfaijin and Ernu Widodo, *Analisis Hukum terhadap Praktik Tindak Pidana Pencucian Uang yang Berasal dari Kejahatan Perjudian*, Jurnal Cendekia Ilmiah, Vol.4, No.3 (2025), p.1971.

In the Indonesian context, traceable fund flows are of critical importance at various stages, including prevention, the reporting of suspicious transactions and evidentiary processes before the courts.[46] Once traceability is removed, the proof of money laundering offences becomes exceedingly difficult. Furthermore, decentralized Crypto Tumblers render the application of Know Your Customer (KYC) or Customer Due Diligence (CDD) principles practically impossible, in contrast to conventional financial service providers and even licensed crypto asset service providers.[47] Decentralized Crypto Tumblers are neither controlled, managed, nor supervised by a clearly identifiable legal entity, thus leaving no legal subject upon whom obligations of user identification or transaction reporting may be imposed. State responses to this phenomenon may vary, whether through the adoption of social-economic policy measures, the formulation of criminal policy, the decision to refrain from regulatory interventions altogether, or the combinations. As a valuable point of reference for assessing the prospective direction of Indonesia's legal policy, the following discussion examines several significant cases involving the use of Crypto Tumblers.

4. Several Landmark Cases on Crypto Tumblers

The regulatory experience of the United States government offers a valuable point of reference for addressing the challenges posed by Crypto Tumblers. Several well-known cases are frequently cited in this context, including Tornado Cash, Bitcoin Fog and Helix. Among these, the Tornado Cash case stands as a particularly significant landmark. Tornado Cash is an Ethereum-based Crypto Tumbler protocol and represents the first decentralized Crypto Mixer to be subjected to legal enforcement in the United States, having been placed under economic sanctions by the Office of the Foreign Assets Control (OFAC) in 2022.[48] Arising from this case,

[46] Dwiki Putra Perkasa, *Op.Cit*..

[47] Azzahra Natazia Ristina Goce, *Model Investasi Cryptocurrency dalam Upaya Pencegahan Tindak Pidana Pencucian Uang*, Mahkamah: Jurnal Riset Ilmu Hukum, Vol.1, No.4 (2024), p.183 dan 186.

[48] Matthias Nadler and Fabian Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers*, Federal Reserve Bank of St. Louis Review, Vol.105, No.2 (2023), p.124.

the Financial Crimes Enforcement Network (FinCEN) of the U.S. proposed amendments to Section 311 of the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act), seeking to impose more stringet obligations on financial institutions to monitor and record transactions suspected of having been processed through digital asset mixing tool.[49]

The FinCEN has proposed amendments to Section 311 of the USA Patriot Act under which digital financial institutions would be required to implement enhanced recording and reporting obligations for transactions involving Crypto Tumblers, particularly cross-border transactions.[50] Failure to comply with these obligations may subject the institutions concerned to civil, administrative and criminal sanctions. Nevertheless, the U.S. faces comparable limitations, as such regulatory measures are effectively applicable only to digital financial asset service providers operating within the CEX structures.[51]

On 21 March 2025, the OFAC removed Tornado Cash from its sanctions list after a court applying the International Emergency Economic Powers Act (IEEPA), held that OFAC had exceeded its statutory authority by imposing sanctions on a ‘smart contract’ (in which it is classified as an intellectual property).[52] This development has reignited speculation regarding the future direction of governmental legal policy and the appropriate stance toward DeFi, particularly whether it signals a shift toward a more accomodative approach or a continued hardline position with respect to decentralized Crypto Tumblers.[53]

---

[49] Financial Crimes Enforcement Network and U.S. Department of the Treasury, *Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern*, Office of the Federal Register, Washington, D.C, 2023, p.6.

[50] David Stier and Eric Hall, *Treasury proposes designating transactions with cryptocurrency mixers a "Primary Money Laundering Concern"*, Retrieved from https://www.dlapiper.com/insights/publications/2023/10/treasury-proposes-designating-transactions-with-cryptocurrency-mixers, Accessed 19 Desember 2025.

[51] NET Bank Audit, *FinCEN Regulation of Virtual Assets and Crypto Mixers: Compliance and Risk Implications for FIs*, Retrieved from https://www.netbankaudit.com/resources/fincen-regulation-of-virtual-assets-and-crypto-mixers, Accessed 19 Desember 2025.

[52] Marcus Wolter and Crystel Saraie, *Tornado Cash: Understanding the Sanctions and Their Implications*, Retrieved from https://caldwelllaw.com/news/tornado-cash-sanctions-lifted-privacy-crypto/, Accessed 2 Januari 2026.

[53] *Ibid*..

The legality of Crypto Tumblers remains a subject of intense debate among crypto users. This debate is driven by the inherent tension between arguments advocating the right to enhance financial privacy and those emphasizing the imperative of preventing money laundering.[54] Both positions rest on defensible normative grounds, as follows.

Proponents of banning Crypto Tumblers argue that efforts to enhance financial anonymity substantially impede transaction traceability for the purpose of anti-money laundering enforcement. Under a regime of outright prohibition, all crypto assets transactions that have passed through a Crypto Tumbler would not only be presumptively classified as suspicious but could also be automatically construed as acts of money laundering. In the contrary, opponents of such prohibition contend that Crypto Tumblers remain necessary instruments for enhancing financial security and privacy for lawful users. Moreover, an outright ban risks imposing disproportionate harm on individuals who utilize Crypto Tumblers for legitimate purposes, including exposure to asset seizure, account freezing, or other coercive enforcement measures. This debate illustrates that a blanket prohibition of Crypto Tumblers does not necessarily yield just or proportionate outcomes.[55]

Aside of Tornado Cash, the U.S. regulatory experience with Crypto Tumblers is further illustrated by the cases of Bitcoin Fog and Helix. Bitcoin Fog was a darknet-based Crypto Tumbler service that operated for more than a decade and was widely used to launder criminal proceeds.[56] Its operator, Roman Sterlingov, was found to have facilitated money laundering derived from a range of predicate crimes, including narcotics trafficking, fraud and cybercrime.[57] Another relevant case is Helix, also a Bitcoin-based darknet Crypto Tumbler operated by Larry Dean Harmon between 2014 and 2017. In total, Helix processed more than 350.000 bitcoins, with an aggregate value exceeding USD 300 millions at the time of the transactions,

[54] Kosta Gushterov, *U.S. Treasury Nears Final Rule to Ban Crypto Mixers*, Retrieved from https://cryptodnes.bg/en/u-s-treasury-nears-final-rule-to-ban-crypto-mixers/, Accessed pada 19 Desember 2025.
[55] Kosta Gushterov, *Op.Cit*..
[56] United States Attorney's Office District of Columbia, *Op.Cit*..
[57] *Ibid*..

the majority of which originated from narcotics trafficking and other illicit activities.[58]

In light of these cases, Crypto Tumblers are not merely susceptible to misuse but have, in practice, become one of the central pillars in dynamics of darknet-based criminal activity. The foregoing cases illustrate that the State cannot adopt a passive stance toward technologies that have been demonstrably used and may continue to be used, as instruments of money laundering. Regulatory inaction toward Crypto Tumblers risks rendering a jurisdiction an attractive haven for criminal actors. Collectively, these cases reinforce the argument that, in the Indonesian context, Crypto Tumblers should not be left unregulated by the State and untouched by the law enforcement actors.

Nevertheless, a fundamental consideration cannot be overlooked: Crypto Tumbler systems, by their very nature, are not amenable to total prohibition, as they operate atop blockchain technologies grounded in mathematical constructions or smart contract basis.[59] As explained earlier in relation to the operational framework of DEX, the functioning of DEX may be analogized to a fictional "currency-exchange vending machine." Such a vending machine is not manually operated by a human administrator; rather, all processes are executed automatically by codes.

In the context of crypto assets, this code is functionally equivalent to a smart contract deployed on a blockchain. Any user may insert a certain amount of funds or coins into the system, which are then processed according to pre-configured code. The output generated by the system cannot be controlled by any individual actor in terms of which specific units are dispensed, as the assets have already been mixed. Consequently, it becomes impossible to determine whether the assets emerging from the system constitute clean or illicit funds. Participants who supply assets into a liquidity pool (commonly referred to in crypto terminology as "liquidity

---

[58] Financial Crimes Enforcement Network, *Harmon Helix Assessment and Statement of Facts*, Financial Crimes Enforcement Network, Washington, D.C, 2020.
[59] Primavera De Filippi and Samer Hassan, *Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code*, First Monday, Vol.21, No.12 (2016), p.10.

providers") are generally regarded as engaging in lawful activity, as such participation is not, in its original conception or by its very nature, considered a criminal act (this logic, however, does not operate conversely).

On that basis, the State cannot simply halt a mathematical formula that is executed automatically by codes and sustained by a decentralized community. Transactions are carried out automatically through smart contracts, rendering traditional assessments of suspicion exceedingly difficult.[60] This very characteristic explains why the State should not automatically classify all transactions routed through Crypto Tumblers as acts of money laundering. In this respect, the State is not positioned to unilaterally prohibit or directly intervene in smart contract-based systems that function across jurisdictions. Accordingly, policy formulation concerning Crypto Tumblers cannot be confined solely to the framework of criminal policy but must be complemented by non-penal approaches that are more responsive and adaptive to technological developments.[61]

Yet such considerations do not diminish the urgency of reformulating criminal policy within the anti-money laundering regime.[62] Criminal policy continues to play as a strategic role, particularly in providing legal certainty for crypto asset users who engage in lawful transactional activities. Resorting to criminal policy, however, should not be equated with the imposition of an outright statutory ban. A total prohibition risks generating significant adverse consequences, not least because technological innovation enables the rapid emergence of alternative platforms that may be even more difficult to tackle, thus potentially producing a perpetual "cat-and-mouse" dynamic between regulators and illicit actors.

---

[60] Muhammad Singgih Imam Wibowo, Akhmad Munawar and Hidayatullah, *Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia Technical and Legal Obstacles in The Investigation Process of Cyber Crimes in Indonesia*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.5, No.7 (2024), p.4.; Trisutrisno Chandra, Akhmad Munawar and Muhammad Aini, *Tinjauan Yuridis terhadap Mekanisme Penyelidikan pada Tindak Pidana Penipuan melalui Media Transaksi Elektronik oleh Kepolisian dalam Sistem Peradilan Pidana di Indonesia*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.5, No.7 (2024), p.13.

[61] Jenny Szabo, Charles Bernard and Laurent Philip, *Legal Implications and Challenges of Blockchain Technology and Smart Contracts*, Computer Life, Vol.12, No.2 (2024), p.8.

[62] Iman Nurjaman and Yuyut Prayuti, *Celah Regulasi Penegakan Hukum dalam Mengatasi Pencucian Uang dari Kejahatan Ekonomi melalui Aset Digital di Indonesia*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.6, No.7 (2025), p.10.

Therefore, the most rational solution within the framework of criminal policy is a graduated prohibition. Such an approach allows for the selective restriction of Crypto Tumblers based on their capacity to incorporate regulatory compliance mechanisms. This may take the form of establishing whitelist of Crypto Tumblers deemed permissible, or imposing conditions under which blockchain-based Tumbler protocols may be regarded as lawful, including the obligation to integrate blockchain analytics providers capable of restricting access by wallet addresses flagged as illicit.[63] This model necessarily entails a synthesis of criminal policy and technological governance, in which Crypto Tumblers that are structurally incapable of adopting compliance measures are progressively prohibited, while those whose protocol design accommodates legal oversight remain permissible. In this manner, criminal policy functions not as a blunt instrument of suppression, but as a "calibrated legal instrument" aimed at mitigating money laundering risks without unduly stifling lawful innovation.

This graduated regulatory prohibition is arguably more appropriate and practicable than an outright prohibition, as it enables the State to mitigate money laundering risks without stifling technological innovation, as affording regulatory space for technological development within the crypto ecosystem may inherently expand economic opportunitites and contribute to the broader growth of the crypto industry as a whole. An outright prohibition would also undermine the State's capacity to enforce the law, given that Crypto Tumblers can and often do, operate on an extraterritorial basis. Accordingly, notwithstanding the continuing importance of criminal policy, reliance on national criminal law frameworks alone is insufficient in light of the inherently cross-jurisdictional nature of both the technology and the conduct associated with it. In this regard, limitations on anonymity (such as through licensing requirements and supervisory oversight by competent authorities, including the Financial Services Authority (OJK) and the Financial Transaction Reports and Analysis Center or PPATK) may be understood as a pragmatic compromise

[63] *Ibid*..

between the protection of financial privacy and the imperatives of law enforcement. Such an approach seeks to curtail excessive anonymity while preserving a financial system that is more resilient to money laundering activities.

C. CONCLUSION

This study finds that the decentralized, automated and cross-jurisdictional nature of smart contract-based systems underlying Crypto Tumbler would make significant obstacles to criminal procedural enforcement under UU TPPU, even KUHAP 2025, making blanket criminalization might be impossible to enforce in practice. Indonesia then should adopt a graduated prohibition model that combines penal and non-penal measures. Rather than imposing an outright ban, the State should implement mechanisms for Crypto Tumblers that incorporate compliance and supervisory requirements. This may be achieved by first, establishing clear criteria for permissible Crypto Tumblers through POJK or other type of internal regulations. Next, OJK should create a whitelist of Tumblers that satisfy such criteria and obtain regulatory approval. Crypto Tumblers that fail to meet these requirements should be prohibited under UU TPPU, while transactions involving their use should be automatically classified as suspicious transactions for monitoring purposes in line with the reports typically issued by PPATK.

REFERENCES

Books

Arief, Barda Nawawi. 2007. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. (Jakarta: Kencana).

Raharjo, Budi. 2022. *Uang Masa Depan: Blockchain, Bitcoin, Cryptocurrencies*. (Semarang: Yayasan Prima Agus Teknik).

Wijaya, Dimaz Ankaa. 2016. *Mengenal Bitcoin dan Cryptocurrency*. (Medan: Puspantara).

Publications

Adwani, Rabail dan V Sudhakar Rao. *Decentralized Finance (DeFi): Reshaping Traditional Banking Systems*. European Economic Letters. Vol.15. No.1 (2025).

Alsalami, Nasser and Bingsheng Zhang. *SoK: A Systematic Study of Anonymity in Cryptocurrencies*. IEEE Conference on Dependable and Secure Computing (2019).

Chandra, Trisutrisno, Akhmad Munawar and Muhammad Aini. *Tinjauan Yuridis terhadap Mekanisme Penyelidikan pada Tindak Pidana Penipuan melalui Media Transaksi Elektronik oleh Kepolisian dalam Sistem Peradilan Pidana di Indonesia*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.5. No.7 (2024).

Filippi, Primavera De and Samer Hassan. *Blockchain Technology as a Regulatory Technology: From Code Is Law to Law Is Code*. First Monday. Vol.21. No.12 (2016).

FinCEN. *Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern*. Federal Register. Vol.88. No.203 (October 2023).

Genkin, Daniel, Dimitrios Papadopoulos and Charalampos. *Privacy in Decentralized Cryptocurrencies*. Communications of the ACM. Vol.61. No.6 (2018).

Goce, Azzahra Natazia Ristina. *Model Investasi Cryptocurrency dalam Upaya Pencegahan Tindak Pidana Pencucian Uang*. Mahkamah: Jurnal Riset Ilmu Hukum. Vol.1. No.4 (2024).

Hermanto, Halim dan Lolita Fitriyana. *Pengaturan Penyitaan Aset Kripto sebagai Hasil Tindak Pidana Pencucian Uang di Indonesia*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.6. No.7 (2025).

Ichsandi, Muhammad Wildan dan Gunardi Lie. *Politik Hukum Digital Banking di Indonesia the Legal Politics of Digital Banking in Indonesia*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.5. No.10 (2025)

Jaiswal, Manishaben. *Cryptocurrency: An Era of Digital Currency*. International Journal of Creative Research Thoughts. Vol.8. No.1 (2020).

Kurfaijin, Satria Angga and Ernu Widodo. *Analisis Hukum terhadap Praktik Tindak Pidana Pencucian Uang yang Berasal dari Kejahatan Perjudian*. Jurnal Cendekia Ilmiah. Vol.4. No.3 (2025).

Kurniawan, I Gede Wahyu Antara, et al.. *The Rise of Decentralized Finance (DeFi): Opportunities for Disruption in Traditional Financial Models*. Journal of Education, Social & Communication Studies. Vol.2. No.2 (2025).

Lin, Lu, Lingyan Han and Liangmin Wang. *A Privacy-Preserving Cross-Chain Cryptocurrency Transfer Scheme Based on Commitment Scheme and Zero-Knowledge Proof*. Computers and Electrical Engineering. Vol.124 (2025).

Moslavac, Bruno. *Cryptocurrency Tumbler: Legality, Legalization, Criminalization*. Revista Acadêmica Escola Superior do Ministério Público do Ceará. Vol.11. No.2 (2019).

Nadler, Matthias and Fabian Schär. *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers*. Federal Reserve Bank of St. Louis Review. Vol.105. No.2 (2023).

Nurjaman, Iman and Yuyut Prayuti. *Celah Regulasi Penegakan Hukum dalam Mengatasi Pencucian Uang dari Kejahatan Ekonomi melalui Aset Digital di Indonesia*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.6. No.7 (2025).

Nwariaku, Harold, et al.. *Blockchain Technology as an Enabler of Transparency and Efficiency in Sustainable Supply Chains*. International Journal of Science and Research Archive. Vol.12. No.2 (2024).

Pakki, Jaswant, et al.. *Everything you Ever Wanted to Know About Bitcoin Mixers (But Were Afraid to Ask)*. Proceedings Financial Cryptography and Data Security: 25th International Conference (FC 2021) .

Perkasa, Dwiki Putra. *Analisis Hukum Kejahatan Ekonomi Digital Cryptocurrency sebagai Instrumen Money Laundering di Indonesia*. RIGGS: Journal of Artificial Intelligence and Digital Business. Vol.4. No.2 (2025).

Permana, Sandhi Bagus. *Legal Policy Concerning the Supervision by the Financial Services Authority Supervisory Board*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.6. No.10 (2025).

Platt, Moritz, dkk.. *Energy Demand Unawareness and the Popularity of Bitcoin: Evidence from Nigeria*. Oxford Open Energy. Vol.2 (2023).

Putra, Tegar San, et al.. *Keabsahan Alat Bukti Digital dalam Pembuktian Kasus Phantom Hacker Scam*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.7. No.7 (2026).

Ridwan, Randa Risgiantana. *Transaksi Mata Uang Virtual (Cryptocurrancy) sebagai Celah Terjadinya Tindak Pidana Pencucian Uang*. Jatiswara: Jurnal Ilmu Hukum. Vol.37. No.3 (2022).

Rosyidah, Hanna, Bayu Satya Ndharma and Naya Aulia Zulfa. *Inkonsistensi Aturan Pertanggungjawaban Pidana Pencucian Uang oleh Korporasi: Perlukan Reformulasi?*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.2. No.12 (2021).

Sari, Adinda Melinia, Sari Mandiana and Paula. *Analisa Pertanggungjawaban Pidana atas Penggunaan Aset Kripto sebagai Sarana Tindak Pidana Pencucian Uang*. Aliansi: Jurnal Hukum, Pendidikan dan Sosial Humaniora. Vol.1. No.2 (2024).

Seres, István András, et al.. *MixEth: Efficient, Trustless Coin Mixing Service for Ethereum*. Proceding International Conference on Blockchain Economics. Security and Protocols (2019).

Szabo, Jenny, Charles Bernard and Laurent Philip. *Legal Implications and Challenges of Blockchain Technology and Smart Contracts*. Computer Life. Vol.12. No.2 (2024).

Thomas, Alejandro Morion Ruben and Happy Yulia Anggraeni. *Cybercrime dan Media Sosial: Analisis Hukum terhadap Tren Peningkatan Tindak Pidana di Era Digital*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.6. No.7 (2025)

Tippe, Pascal and Christoph Deckers. *Unmixing the Mix: Patterns and Challenges in Bitcoin Mixer Investigations*. Forensic Science International: Digital Investigation. Vol.52 (2025).

Wibowo, Muhammad Singgih Imam, Akhmad Munawar and Hidayatullah. *Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia Technical and Legal Obstacles in The Investigation Process of Cyber Crimes in Indonesia*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.5. No.7 (2024).

Wu, Lei, et al.. *Towards Understanding and Demystifying Bitcoin Mixing Services*, *Towards Understanding and Demystifying Bitcoin Mixing Services*. Proceedings of The Web Conference (2021).

Scholarly Works

Chan, laine and Sion Yoong Tian. 2022. *The Rise of Decentralised Finance (DeFi): Opportunities for Disruption in Traditional Financial Models*. (London: LexisNexis).

Aquilina, Matteo, et al.. 2024. *Decentralised Dealers? Examining Liquidity Provision in Decentralised Exchanges*. Working Paper. Basel: Bank for International Settlements.

Website

FATF. *The Fath is Leading Global Action to Fight Back*. Retrieved from https://www.fatf-gafi.org/en/the-fatf/what-we-do.html. Accessed 26 Desember 2025.

Febriani, Sekar. *Indonesia Peringkat ke-7 Dunia untuk Adopsi Kripto, Total Transaksi Sentuh Rp 360 Triliun*. Retrieved from https://www.liputan6.com/crypto/read/6201340/indonesia-peringkat-ke-7-dunia-untuk-adopsi-kripto-total-transaksi-sentuh-rp-360-triliun?page=3#google_vignette. Accessed 19 Desember 2025.

Gushterov, Kosta. *U.S. Treasury Nears Final Rule to Ban Crypto Mixers*. Retrieved from https://cryptodnes.bg/en/u-s-treasury-nears-final-rule-to-ban-crypto-mixers/. Accessed 19 Desember 2025.

NET Bank Audit. *FinCEN Regulation of Virtual Assets and Crypto Mixers: Compliance and Risk Implications for FIs*. Retrieved from https://www.netbankaudit.com/resources/fincen-regulation-of-virtual-assets-and-crypto-mixers. Accessed 19 Desember 2025.

Stier, David and Eric Hall. *Treasury proposes designating transactions with cryptocurrency mixers a "Primary Money Laundering Concern"*. Retrieved from https://www.dlapiper.com/insights/publications/2023/10/treasury-proposes-designating-transactions-with-cryptocurrency-mixers. Accessed 19 Desember 2025.

United States Attorney's Office District of Columbia. *Operator of 'Bitcoin Fog' Sentenced to More Than 12 Years in Prison for Running Notorious Darknet Cryptocurrency Mixer*. Retrieved from https://www.justice.gov/usao-dc/pr/operator-bitcoin-fog-sentenced-more-12-years-prison-running-notorious-darknet. Accessed 22 Desember 2025.

Wolter, Marcus and Crystel Saraie. *Tornado Cash: Understanding the Sanctions and Their Implications*. Retrieved from https://caldwelllaw.com/news/tornado-cash-sanctions-lifted-privacy-crypto/. Accessed 2 Januari 2026.

Legal Sources

Undang-Undang Nomor 1 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana.

Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 27 Tahun 2024 tentang Penyelenggaraan Perdagangan Aset Keuangan DigitalTermasuk Aset Kripto.

Other Sources

Financial Action Task Force. 2014. *Virtual Currencies-Key Definitions and Potential AML/CFT Risks*. Paris: Financial Action Task Force.

Financial Action Task Force. 2025. *Best Practices on Travel Rule Supervision*. Paris: Financial Action Task Force.

Financial Action Task Force. 2025. *Explanatory Note for Revised Recommendation 16 (R.16)*. Paris: Financial Action Task Force.

Financial Crimes Enforcement Network. 2020. *Harmon Helix Assessment and Statement of Facts*. Washington, D.C.: Financial Crimes Enforcement Network.

Financial Crimes Enforcement Network and U.S. Department of the Treasury. 2023. *Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern*. Washington, D.C: Office of the Federal Register.

Karunian, Alia Yofira, Muhammad Tanziel Aziezi and Seira Tamara Herlambang. 2024. *Unraveling the Vulnerabilities of Abuse and Enforcement of Digital Currency Related to Criminal Offenses*. Jakarta: Indonesian Corruption Watch.

United States Department of Justice. *What Is the Patriot Act?*. Washington, D.C.: United States Department of Justice.

World Bank Group. 2018. *Cryptocurrencies and Blockchain*. Washington, D.C.: World Bank Group.