AL RISALAH: Jurnal Ilmu Syariah dan Hukum

VOLUME 26 NO 1, MAY 2026
P-ISSN: 2252-8334 / E-ISSN: 2550-0309

https://doi.org/10.24252/al-risalah.vi.63015

Legal Analysis of the Use of Decentralized Exchange (DEX) in Digital Money Laundering Schemes

Lavia Luky Carolina[1*], Abdul Kholiq[2]
[1]*E-mail : 2210611078@mahasiswa.upnvj.ac.id*
[2]*E-mail : abdulkholiq@upnvj.ac.id*
[1,2]*Universitas Pembangunan Nasional Veteran Jakarta, Indonesia*
*corresponding author

Article history:
Submission: 18 October 2025
Received in revised form: 26 Nopember 2025
Acceptance date: 07 December 2025
Available online: 21 December 2025

Keywords:
Cryptocurrency; Decentralitation; Money Laundering; Regulation Indonesia.

How to Cite:
Carolina, L. L., & Kholiq, A. (2025). Legal Analysis of the Use of Decentralized Exchange (DEX) in Digital Money Laundering Schemes . Al-Risalah Jurnal Ilmu Syariah Dan Hukum.
https://doi.org/10.24252/al-risalah.vi.63015

Abstract
The use and transaction of crypto assets in Indonesia have grown massively as a form of innovation in digital finance. However, as with any technological advancement, this progress also brings challenges, particularly the risk of crypto assets being misused for money laundering through Decentralized Exchanges (DEX). This study aims to analyze legal certainty and the obstacles to enforcing anti–money laundering (AML) regulations in DEX transactions, which operate outside the supervision of any centralized authority. This research employs a normative juridical method through statutory and conceptual approaches to assess the adequacy of national regulations, particularly the Anti–Money Laundering Law (UU TPPU) and POJK Number 27 of 2024. The findings reveal regulatory gaps, user anonymity, and the cross-jurisdictional nature of DEX transactions, all of which complicate tracing and evidence collection. The study recommends establishing a comprehensive regulatory framework for digital assets, strengthening oversight through legally reachable entities such as centralized exchanges (CEX), wallets, and on–off-ramp services, as well as enhancing the capacity of law enforcement in blockchain forensics to improve the effectiveness of AML enforcement.

INTRODUCTION

Entering the 21st century, technological development has brought significant transformations to various aspects of human life; the progress and development of the industrial revolution have brought about economic and social changes. The term "development" implies an impact on "revolution," which indicates the rapidity of said development.[1] Digital innovation has given rise to new forms of transactions and economic value that are no longer fully reliant on conventional money. One of the most influential innovations is cryptocurrency. Despite being an advancement in the financial sector, this technology simultaneously presents new challenges, particularly within the context of law enforcement. Existing loopholes are frequently exploited by criminals to develop new *modi operandi* for criminal acts. In this regard, the criminal act of money laundering has not escaped the exploitation of these loopholes, considering that its anonymous and decentralized nature can complicate the process of tracing illicit fund flows.

Money laundering in Indonesia is regulated under Law Number 8 of 2010 concerning the Prevention and Eradication of the Criminal Act of Money Laundering (UU TPPU). The Act defines money laundering through various actions such as placing, transferring, spending, converting, or exchanging assets known or reasonably suspected to constitute proceeds of crime, with the intent of concealing or disguising their unlawful origin. This demonstrates that TPPU involves manipulative efforts designed to make illicit assets appear legitimate.

In the Indonesian legal framework, crypto assets are classified as commodities rather than currency, and therefore cannot serve as legal tender. BAPPEBTI Regulation No. 13 of 2022 defines crypto assets as intangible commodities utilizing cryptography, peer-to-peer networks, and distributed ledger technology. Meanwhile, Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector and Law No. 7 of 2011 on Currency reaffirm that the Rupiah is the only lawful means of payment in Indonesia. Accordingly, Bank Indonesia prohibits the use of cryptocurrency as an official payment instrument, primarily due to concerns surrounding consumer protection, risk mitigation, and macroeconomic stability.risk mitigation, and the necessity of safeguarding national macroeconomic stability.

[1] Yati Nurhayati et al., "The Issue of Copyright Infringement in 4.0 Industrial Revolution: Indonesian Case," *Jurnal Media Hukum*, 2019, 122–30.

In Indonesia, public interest in crypto assets has experienced rapid growth in recent years. Based on data from the Commodity Futures Trading Regulatory Agency (Bappebti), the Financial Services Authority (OJK) stated that total crypto asset transactions reached IDR 650 trillion as of December 2024 in Indonesia. Every day, crypto assets amounting to IDR 2 trillion are transacted.[2] These figures indicate that crypto adoption has become a phenomenon that cannot be disregarded, particularly concerning the formulation of regulation and legal protection. Crypto asset transaction exchanges themselves consist of two types, namely Centralized Exchange (CEX) and Decentralized Exchange (DEX).

A Centralized Exchange (CEX) is a transaction platform that facilitates the trading of crypto assets through a centralized intermediary, wherein the platform operator functions as the intermediary, serving as the transaction organizer, asset custodian, and clearing house, utilizing an order book as the pricing mechanism. Users can exchange crypto assets with one another without needing to access their own private keys.[3] Conversely, a Decentralized Exchange (DEX) is a crypto asset transaction platform built using a distributed ledger or similar technology, where transactions can occur directly between crypto asset customers,[4] and can only be identified by a numeric code, although sometimes they can also be associated with pseudonyms. Consequently, the absence of AML (Anti-Money Laundering) regulation and KYC (Know Your Customer) mechanisms gives rise to the risk of the criminal act of money laundering being committed by Bitcoin users.[5] A DEX is a crypto exchange that permits users to trade assets directly without an intermediary. No party custodies the user's funds, and transactions are executed via smart contracts.

Therefore, it is not only a matter of regulation and legal certainty that has not robustly encompassed DEX; the anonymous nature of the platform and the absence of reporting obligations related to suspicious transactions pose a substantial challenge for law enforcement officials, particularly the PPATK (Financial Transaction Reports and Analysis Center), in conducting tracing and tracking fund flows. This condition massively impedes the prevention and enforcement of laws against the practice of money laundering crimes via DEX. Considering the complexity of modern digital crime, the law

[2] Tempo, "OJK Sebut Transaksi Kripto Tembus Rp 650 Triliun per Desember 2024, Apa Itu Aset Kripto?," Tempo.co.id, 2024, https://www.tempo.co/ekonomi/ojk-sebut-transaksi-kripto-tembus-rp-650-triliun-per-desember-2024-apa-itu-aset-kripto--1207251 .
[3] Bank for International Settlements, *The Crypto Ecosystem : Key Elements and Risks*, 2023.
[4] Bank for International Settlements.
[5] Anastasya Dowongi, "Implementasi Hukum Mengenai Tindak Pidana Pencucian Uang (Money Launderyng) Menurut Undang-Undang No 8 Tahun 2010," *Lex Privatum* 13, no. 5 (2024).

must not succumb to stagnation. As the adage states, *Lex semper dabit remedium* (The law will always provide a remedy), this research is present to break through said impasse.

METHOD

The research method utilized in this study is the normative legal research methodology.[6] This research focuses on the analysis of the legal framework and doctrines pertaining to the utilization of Decentralized Exchange (DEX) within digital money laundering criminal schemes. This study employs a statute approach by analyzing regulations pertaining to the criminal act of money laundering, information technology, and the financial system. And a conceptual approach, which is utilized to comprehend crucial concepts such as cryptocurrency, decentralized exchange, digital money laundering, transaction anonymity, as well as regulations and policies in the field of digital finance. This study utilizes primary legal materials which include Law Number 8 of 1981 concerning the Criminal Procedure Code, Law Number 8 of 2010 concerning the Prevention and Eradication of the Criminal Act of Money Laundering, Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector, BAPPEBTI (Commodity Futures Trading Regulatory Agency) Regulations and POJK (Financial Services Authority) Regulations; secondary legal materials include journals, books, and research findings; and tertiary legal materials include legal encyclopedias and legal dictionaries. The data collection method is conducted through library research or a documentation study of relevant statutory regulations and legal literature. Data analysis is performed using an analytically descriptive method by employing deductive reasoning, namely by drawing conclusions from legal principles that are general in nature (general) towards their specific application (specific) within the context of crypto assets and DEX.

RESULTS AND DISCUSSION

1. Regulation and Legal Certainty Pertaining to the Practice of Money Laundering Through Decentralized Exchanges

Cryptocurrency, or crypto assets, has currently become a trend, wherein Indonesia constitutes one of the largest countries of crypto asset users in the world. The crypto asset ecosystem in Indonesia continues to experience rapid growth. As of September 2025, the Financial Services Authority (OJK) recorded that the number of national crypto asset users reached 18.61 million consumers, with total transactions amounting to more than IDR 360 trillion. The growth in the number of users continues to increase consistently,

[6] Peter Mahmud Marzuki, *Penelitian Hukum: Edisi Revisi* (Prenada Media, 2017).

with a month-to-month increase reaching 3-5%. Based on a report released by Chainalysis, Indonesia ranks seventh out of 151 countries in the 2024 Global Crypto Adoption Index. This achievement affirms Indonesia's position as one of the most developing crypto markets in the world, whilst simultaneously demonstrating the high level of public adoption and participation in the global crypto asset ecosystem.[7]

Crypto assets constitute a digital or virtual currency that is secured by cryptography. In Indonesia, POJK (OJK Regulation) Number 27 of 2024, Article 1 number 6, defines crypto assets as a digital representation of value that can be stored and transferred utilizing technology that enables the use of a distributed ledger, such as blockchain, to verify its transactions and ensure the security and validity of the stored information; is not guaranteed by a central authority such as a central bank but is issued by private parties; can be transacted, stored, and moved or transferred electronically; and can be in the form of digital coins, tokens, or other asset representations which include backed crypto-assets and unbacked crypto-assets.[8]

In Indonesia, crypto assets are categorized as a commodity, previously supervised by BAPPEBTI (Commodity Futures Trading Regulatory Agency), pursuant to BAPPEBTI Regulation Number 13 of 2022 and Number 4 of 2023, which regulate the governance of commodity futures trading as well as the list of crypto assets that are legal to be traded. However, effective January 10, 2025, the supervisory authority was transferred from BAPPEBTI to the Financial Services Authority (OJK) based on Article 8 number 4 and Article 312 paragraph (1) of Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector. As a follow-up action, OJK stipulated POJK Number 27 of 2024 concerning the Implementation of Digital Financial Asset Trading including Crypto Assets, which has become the latest legal basis for the regulation and supervision of crypto assets in Indonesia.

The Criminal Act of Money Laundering (TPPU) is regulated in Law Number 8 of 2010 concerning the Prevention and Eradication of the Criminal Act of Money Laundering; its implementation and supervision are carried out by the PPATK (Financial Transaction Reports and Analysis Center). An act is classified as TPPU if it fulfills the elements stipulated in Article 3, Article 4, and Article 5 of the aforementioned Law. The Criminal Act of Money Laundering itself is a crime that possesses a distinct characteristic;

[7] Sekar Febriani, "Indonesia Peringkat Ke-7 Dunia Untuk Adopsi Kripto, Total Transaksi Sentuh Rp 360 Triliun," Liputan6.com, 2025, https://www.liputan6.com/crypto/read/6201340/indonesia-peringkat-ke-7-dunia-untuk-adopsi-kripto-total-transaksi-sentuh-rp-360-triliun.
[8] *Peraturan Otoritas Jasa Keuangan Nomor 27 Tahun 2024 Tentang Penyelenggaraan Perdagangan Aset Keuangan Digital Termasuk Aset Kripto*, n.d.

specifically, this crime is not a singular crime but rather a dual crime. Money laundering is a crime that is inherently a *follow-up crime*, whereas the principal crime or original crime is referred to as a *predicate offense* or *core crime*, or in some jurisdictions, it is formulated as an *unlawful activity*, namely the original crime that yields the money which is subsequently subjected to the money laundering process.[9]

Several acts categorized as criminal acts of money laundering under the TPPU Law include:

a. Placing, transferring, spending, paying, granting (hibah), donating (sumbang), depositing (menitipkan), or changing the form of assets that are known or reasonably suspected to be derived from the proceeds of a criminal act with the objective of disguising their origin;
b. Concealing or disguising the origin, source, location, designation, ownership, or rights to assets that are known or reasonably suspected to be derived from the proceeds of a criminal act;
c. Receiving or controlling assets that are known or reasonably suspected to be derived from the proceeds of a criminal act;
d. Assisting or conspiring with other parties in committing money laundering, including providing facilities to disguise or conceal the proceeds of crime; and
e. Utilizing assets derived from the proceeds of a criminal act for business activities or financial transactions to evade detection by authorized authorities.

Based on the anti-money laundering law, the acts qualified as criminal acts consist of two matters:

a. The criminal act of money laundering as regulated in Article 3 through Article 10; and
b. Other criminal acts related to the criminal act of money laundering as regulated in Article 11 through Article 16.[10]

Article 3 of the TPPU Law can be used to ensnare an individual who places, moves, or transfers crypto assets originating from criminal acts through a crypto asset trading platform registered in Indonesia. However, at present, the Law does not yet explicitly include blockchain-based digital assets as an object of the criminal act of TPPU. This creates a legal loophole that is susceptible to exploitation by perpetrators of economic

[9] Dowongi, "Implementasi Hukum Mengenai Tindak Pidana Pencucian Uang (Money Launderyng) Menurut Undang-Undang No 8 Tahun 2010."
[10] Ryan Keynes Bidjuni, Ramdhan Kasim Kasim, and Dince Aisa Kodai, "Penegakan Hukum Terhadap Tindak Pidana Pencucian Uang Melalui Cryptocurrency Di Indonesia," *Gorontalo Justice Research* 1, no. 1 (2025): 208–18.

crimes. They can utilize crypto assets for the *placement* and *layering* stages of the proceeds of crime, with a low risk of detection by the prevailing financial transaction reporting systems.

In the world of cryptocurrency, there are two main types of exchanges, namely Centralized Exchange (CEX) and Decentralized Exchange (DEX). A Centralized Exchange (CEX) is a centralized trading platform that involves an intermediary in facilitating crypto asset transactions. The CEX operator acts as the central party to organize transactions, store assets (custody), and perform clearing, while using an order book mechanism to determine prices. By using a CEX, users can easily exchange crypto assets with each other without needing to access or manage their own private keys.[11] Whereas, a Decentralized Exchange (DEX) is a crypto asset transaction platform built using a distributed ledger or similar technology where transactions can occur directly between crypto asset customers,[12] and can only be identified by numeric codes, but sometimes can also be associated with pseudonyms. Consequently, the absence of AML (Anti-Money Laundering) regulation and KYC (Know Your Customer) mechanisms causes a risk of the criminal act of money laundering that can be committed by Bitcoin users.[13] A DEX is a crypto exchange that allows users to trade assets directly without an intermediary or peer-to-peer. No party custodies the user's funds, and transactions are executed with smart contracts.

Regulation related to crypto assets is found in several regulations; for example, BAPPEBTI Regulation No. 13 of 2022 concerning Guidelines for the Operation of Physical Market Trading of Crypto Assets (Crypto Asset) on the Futures Exchange, in Article 2 regulates that the physical market trading of crypto assets may only be conducted by Physical Crypto Asset Traders who have obtained a license from Bappebti and are obligated to implement KYC, AML, and CFT (Combating the Financing of Terrorism) principles.[14] Meanwhile, Minister of Trade Regulation Number 99 of 2018 concerning the General Policy for the Operation of Crypto Asset Futures Trading, in Article 2, affirms that crypto trading may only be conducted on a futures exchange that has been approved by BAPPEBTI. Crypto assets are classified as a digital commodity according to Law No. 10 of 2011 juncto Law No. 32 of 1997 concerning Commodity Futures Trading, not as a means of payment.

---

[11] Bank for International Settlements, *The Crypto Ecosystem : Key Elements and Risks*.
[12] Bank for International Settlements.
[13] Paskalis Jovena Limaatmaja, "Aspek Pidana Terhadap Transaksi Mata Uang Kripto Yang Berpotensi Sebagai Tempat Pencucian Uang" 2, no. 4 (2024): 511–32.
[14] *Peraturan BAPPEBTI No. 13 Tahun 2022 Tentang Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (Crypto Asset) Di Bursa Berjangka*.

However, with the transfer of supervisory authority over crypto assets from BAPPEBTI to the OJK, future regulation will be guided by regulations stipulated through POJK (OJK Regulations). If referring to POJK Number 27 of 2024, Article 3 paragraph (2), it is stated that operators of digital financial asset trading are obligated to apply principles of good governance, risk management, market integrity, information system security, consumer protection, as well as the prevention of TPPU (Money Laundering), TPPT (Terrorist Financing), and PPSPM (Proliferation of Weapons of Mass Destruction Financing), personal data protection, and finally, fulfillment of statutory regulation provisions. This provision can be interpreted that this regulation is intended for crypto exchanges that have a centralized authority, thereby obligating them to follow the provisions within the POJK, subject to the regulatory provisions. This provision is clearly aimed at operators that possess an institutional form and are under the supervision of the OJK, namely centralized (CEX) crypto asset trading platforms. CEX exchanges themselves implement KYC and AML systems as regulated in the OJK provisions and other implementing regulations. This contrasts with a DEX, which operates without a central authority and does not have a legal entity that can be held accountable. A DEX runs automatically via smart contracts and has no reporting obligations or supervision over transaction activities. Consequently, this POJK normatively only regulates licensed and supervised CEXs, while DEXs still remain outside the reach of formal regulation.

Efforts to strengthen legal certainty in handling cryptocurrency-based TPPU must begin with regulatory updates focused on the clarity of the legal status of digital assets and regulation of entities directly connected to the DEX ecosystem. Considering that DEXs are decentralized and lack a central authority, direct regulation of DEX protocols is unrealistic and potentially conflicts with the nature of the technology. Indonesia does not need to force the creation of regulations that bind DEX protocols. Therefore, national regulatory revisions must be directed at affirming the legal definition of cryptocurrency within the context of criminal acts, including its standing as an object of seizure, evidentiary proof, and part of the asset recovery mechanism. On the other hand, effective supervision is conducted through the entities that serve as the entry-exit points (on-ramps and off-ramps) for value towards DEXs, namely CEXs, wallets, and on-off ramp services, and the utilization of Blockchain Analytics. Through the strengthening of KYC obligations, the application of the *travel rule*, automated reporting mechanisms, and data integration with the PPATK, the state can still monitor the flow of value heading to DEXs without intervening in the decentralized nature of the protocol itself. This approach ensures that Indonesia regulates aspects that are factually reachable by law, yet still preserves the space for innovation within the digital financial ecosystem.

As a follow-up to strengthening supervision, Indonesia needs to establish a special institution or task force that functions to oversee criminal acts via digital assets in a coordinated and responsive manner. The character of digital asset-based crime, which is cross-sectoral and technology-based, demands solid coordination among the PPATK, OJK, Bappebti, Kominfo (Ministry of Communication and Informatics), and law enforcement officials. Through a structured task force, the processes of detection, blockchain analysis, digital forensic investigation, through to enforcement can be conducted in an integrated manner and no longer stop at the sectoral boundaries of each respective institution. The establishment of this special institution can also become a primary pillar in the implementation of a digital asset law that will function as a national legal umbrella (*payung hukum*), harmonizing the various sectoral regulations that have thus far operated independently. With these two main steps, strengthening regulation on DEX-related entities and establishing a special institution, Indonesia can present a legal framework that is modern, adaptive, and provides legal certainty in facing the risks of TPPU through digital assets.

2. Challenges in the Prevention and Application of Law Against the Criminal Act of Money Laundering Through Decentralized Exchange Transactions

Crypto Assets are not a new phenomenon for society; their utilization is already quite massive in Indonesia and is no longer merely an investment instrument but also an integral part of the digital economy ecosystem. However, their virtual, dynamic, and blockchain-technology-based nature opens significant potential for misuse as a medium for the Criminal Act of Money Laundering (TPPU). There are two well-known types of crypto asset exchanges: Centralized Exchange (CEX) and Decentralized Exchange (DEX). CEX is a type of exchange that is centralized, which means its operations are under a central management authority. As a centralized entity, CEX is obligated to comply with prevailing regulations, such as POJK (OJK Regulations), and is under the supervision of the OJK (Financial Services Authority). Compliance with these regulations requires CEX to implement KYC (Know Your Customer) and AML (Anti-Money Laundering) systems. This is regulated in POJK Number 27 of 2024, such that if suspicious transaction activity suspected of being the criminal act of money laundering occurs, it can be reported to the PPATK (Financial Transaction Reports and Analysis Center). With this regulation, authorities can trace crypto assets originating from criminal acts through the user's identity recorded on said platform. However, it is a different matter if the perpetrator utilizes Decentralized Exchanges (DEX) or private wallets, where transactions are executed by smart contracts that do not require user identification, thereby complicating

law enforcement efforts, especially when transactions are executed abroad.[15] DEX is a *trustless* platform run entirely by smart contracts, meaning there is no managing party that stores user data or controls the traded assets.[16] Consequently, conventional AML mechanisms such as KYC obligations, Suspicious Transaction Reports (STR), and record keeping cannot be effectively applied. This loophole is exploited by criminals to conduct the *placement* and *layering* stages in the money laundering process. For example, perpetrators can move the proceeds of crime from private wallets to various DEXs, exchange them for other crypto assets through cross-chain swaps, or obfuscate the transaction trail using *mixers* and *privacy coins*.[17]

In addition to its anonymous nature, another challenge arises because transactions on DEX are global and cross-jurisdictional, complicating prevention processes. The network nodes and liquidity providers are dispersed across various countries, meaning no single authority possesses sole jurisdiction over all activities occurring therein. This condition makes the process of supervising the flow of crypto assets extremely difficult to conduct.[18] On the other hand, institutions such as the Financial Transaction Reports and Analysis Center (PPATK) face limitations in conducting analysis of blockchain-based transactions, because the on-chain tracing process requires sophisticated forensic technology tools as well as technical expertise that law enforcement officials do not yet fully possess.[19]

In addition to technical factors, normative aspects also pose a significant obstacle. National regulation in Indonesia, specifically Law Number 8 of 2010 concerning the Prevention and Eradication of the Criminal Act of Money Laundering, in Article 3 reads: "Any person who places, transfers, conveys, spends, pays, grants (hibah), deposits (menitipkan), carries abroad, changes the form, exchanges for currency or securities or commits other acts upon Assets which he/she knows or reasonably suspects are the proceeds of a criminal act as referred to in Article 2 paragraph (1) with the objective of concealing or disguising the origin of the Assets shall be sentenced for the criminal act of Money Laundering with a maximum imprisonment of 20 (twenty) years and a maximum

[15] Tiara Putri et al., "Inadequate Cryptocurrency and Money Laundering Regulations in Indonesia (Comparative Law of US and Germany)," *Yustisia* 12, no. 2 (2023): 129–52.
[16] Sascha Hägele, "Centralized Exchanges vs. Decentralized Exchanges in Cryptocurrency Markets: A Systematic Literature Review," *Electronic Markets* 34, no. 1 (2024): 33.
[17] Hägele.
[18] Semyon Malamud and Marzena Rostek, "Decentralized Exchange," *American Economic Review* 107, no. 11 (2017): 3320–62.
[19] Asmara Nova Susanto and Wiwik Afifah, "Peran Lembaga Yang Mendukung Penelusuran Alat Bukti Tindak Pidana Pencucian Uang Yang Menggunakan Cryptocurrency," *Media Hukum Indonesia (MHI)* 2, no. 4 (2024).

fine of IDR 10,000,000,000.- (ten billion rupiah)".[20] Thus, any act that fulfills every element stipulated in Article 3 is included in the criminal act of money laundering.

In the context of crypto assets, although these elements appear clear and are theoretically applicable, in practice, law enforcement still faces difficulties in proving the elements to ensnare TPPU perpetrators. The primary challenge is the nature of anonymity and decentralization of crypto, which complicates the tracing of the perpetrator's identity as well as the recipient of the assets.

From the perspective of evidentiary proof, the most classic challenge is linking pseudonymous blockchain addresses to real-world legal subjects and subsequently proving the connection between the digital assets and the *predicate crime*. Although the blockchain stores a transaction record that is public, said record indicates the flow of value between addresses, not the identity of the address owners. Thus, it requires off-chain evidence. For example, KYC data from a CEX, fiat-on/off ramp service providers, or communication evidence is needed to link an address to a person or legal entity.[21] Without this off-chain evidence, the subjective element and the causal link to the predicate crime are often difficult to fulfill under the standards of proof in criminal law.

The cross-border jurisdictional aspect adds complexity. Digital assets can move between protocols and between jurisdictions in a matter of minutes via cross-chain bridges or cross-network swaps, rendering information requests through conventional MLA (Mutual Legal Assistance) procedures delayed and ineffective for the purpose of freezing or seizing assets before said assets disappear into other jurisdictions or to addresses utilizing privacy technology. The legal gap between countries in defining who constitutes a Virtual Asset Service Provider (VASP) and how to apply the *travel rule* creates opportunities for *regulatory arbitrage* for perpetrators who migrate their operations to jurisdictions with weak supervision.

Institutional capacity constitutes a real obstacle: law enforcement officials and financial intelligence agencies in many jurisdictions still lack the resources, analytical tools, and human resources (SDM) capable of analyzing multi-chain flow patterns and interpreting on-chain evidence. Blockchain forensic training, the procurement of sophisticated analytical tools, and the establishment of special cyber-finance units become prerequisites for investigations to run effectively. Cooperation with private

[20] Amelia Khairunisa and Atik Winanti, "Batasan Usia Dewasa Dalam Melaksanakan Perkawinan Studi Undang-Undang Nomor 16 Tahun 2019," *JUSTITIA: Jurnal Ilmu Hukum Dan Humaniora* 8, no. 8 (2021): 774–84, http://jurnal.um-tapsel.ac.id/index.php/Justitia%7C.
[21] Author Emma Oye, Joyce Walker, and Victoria Smith, "The Role of Decentralized Exchanges (DEXs) in Money Laundering Schemes," no. August (2025).

blockchain analytics providers accelerates the process of identifying patterns, but it also creates a dependency on third parties and raises issues related to methodological transparency and data access.[22]

As a legal response, several policy dilemmas emerge that must be addressed carefully. A legislative approach that expands the definition of VASP or imposes KYC obligations on DEX infrastructure providers may close some loopholes, but it risks damaging the principles of decentralization and privacy that are the objectives of said technology. Therefore, many regulators are adopting a *risk-based approach* and directing enforcement measures at controllable points while encouraging the development of voluntary compliance standards within the DeFi community.[23] Furthermore, the formulation of new legal instruments, such as expedited orders for on-chain asset freezing, cross-border recognized address tagging policies for criminal proceeds, and rapid response mechanisms between FIUs (Financial Intelligence Units), are deemed necessary to close the temporal gap between the criminal act and the enforcement response.[24]

Several developed countries have demonstrated significant progress in building a comprehensive regulatory system for cryptocurrency. We can observe regulations from other countries; for example, Singapore has become one of the more proactive developed nations by introducing the Payment Services Act (PSA), which provides a clear legal framework related to digital payment services, including cryptocurrency. The Monetary Authority of Singapore (MAS), as the primary regulator, has mandated digital asset service providers to comply with AML and KYC standards.[25] In the United States, the regulatory approach is multi-agency and functional. FinCEN classifies businesses providing exchange/transfer services for *convertible virtual currency* (CVC) as Money Services Businesses (MSB) under the Bank Secrecy Act, consequently, entities performing transfer or exchange functions are required to register, establish an AML program, and report suspicious transactions; at the same time, the SEC and CFTC assess tokens/activities based on securities or commodities criteria, thus supervisory authority may differ depending on the token's function and the service. This practice triggers enforcement focused on the fiat-on/off ramp integration points and operators providing custodial or off-chain services. Singapore adopts a pragmatic legislative framework. The

[22] Susanto and Afifah, "Peran Lembaga Yang Mendukung Penelusuran Alat Bukti Tindak Pidana Pencucian Uang Yang Menggunakan Cryptocurrency."
[23] FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Paris: FATF, 2021).
[24] Oye, Walker, and Smith, "The Role of Decentralized Exchanges (DEXs) in Money Laundering Schemes."
[25] Monetary Authority of Singapore (MAS), *Payment Services Act 2019* (Singapore: Monetary Authority of Singapore (MAS), 2020), https://www.mas.gov.sg.

Payment Services Act (PSA) classifies Digital Payment Token services and requires licensing and the application of AML/KYC for digital asset service providers. The MAS authority also urges the use of blockchain analysis technology for supervision and, since 2025, has tightened rules related to cross-border promotions for retail investor protection. The Singaporean approach exemplifies how a small country with an advanced fintech ecosystem combines licensing, technical supervision, and enforcement to limit misuse. The PSA regulates cryptocurrency service providers to comply with Anti-Money Laundering (AML) and Know Your Customer (KYC) principles. In the practice of enforcement against DeFi/DEX entities, global authorities tend to adopt a function-based approach. If a platform or the party behind it performs functions equivalent to a VASP (custody, off-chain matching, running a relayer, receiving fees/treasury), then said entity can be subjected to registration and AML obligations. Conversely, DEXs that are fully *permissionless* and lack an identifiable legal entity remain a regulatory challenge, such that law enforcement typically targets integration points like bridges, fiat gateways, CEXs providing on/off ramps, and tangible fee-earning service providers. This is also noted in comparative studies which show that countries with more mature frameworks target these integration points for supervisory effectiveness.

The regulative practices of these countries reinforce that the main challenges in the prevention and application of law against the criminal act of money laundering through DEX stem from user anonymity, decentralization without a central authority, and the cross-jurisdictional nature of transactions. The complexity of blockchain technology renders conventional proof and supervision mechanisms inadequate, while the limited authority of law enforcement officials exacerbates the ineffectiveness of enforcement. Therefore, Indonesia needs to adopt an approach that aligns with international practice, namely not forcing direct regulation upon DEX protocols, but rather developing proactive regulations that target entities factually connected to DEXs, such as CEXs, wallets, and on-off ramp services. This approach must be accompanied by an affirmation of the legal status of cryptocurrency, the strengthening of KYC obligations, the application of the *travel rule*, data integration with the PPATK, and the utilization of blockchain analytics to trace suspicious asset movements. Furthermore, the establishment of a special digital asset task force and the harmonization of regulations through a digital asset law are necessary to improve cross-institutional coordination and provide comprehensive legal certainty. With these steps, Indonesia can build a legal system that is adaptive, modern, and effective in facing the risks of TPPU through DEX transactions without stifling innovation in the digital financial ecosystem.

CONCLUSION

This research demonstrates that the primary issue in the practice of the criminal act of money laundering via Decentralized Exchange (DEX) lies in the incompatibility between the fundamental character of DEX and the prevailing regulatory structure in Indonesia. The research findings reveal that the entire existing legal framework—such as the TPPU Law (Money Laundering Law), the P2SK Law (Financial Sector Development and Strengthening Law), Bappebti regulations, and POJK 27/2024—structurally can only be enforced against centralized entities, such as a Centralized Exchange (CEX). Meanwhile, a DEX possesses no legal entity, does not perform custodial functions, does not have an operator who can be held accountable, and is not obligated to implement KYC, AML, and suspicious transaction reporting. This finding constitutes the most important result of the research, as it demonstrates that the regulatory incapacity is not merely a technical issue or an issue of transaction anonymity, but rather a fundamental problem in the form of a regulatory blind spot that arises from the structural divergence between the national legal system and the decentralized financial ecosystem. Without this research, the systematic relationship between the operational nature of DEX and the weakness of legal certainty pertaining to TPPU would not be clearly apparent. In answering the research questions, the theory and methods utilized proved to be adequate. The normative approach through the *statute approach* and the *conceptual approach* was capable of accurately mapping the boundaries of Indonesia's regulatory authority as well as explaining the challenges of legal application to DEX transactions. For the first research question, this method affirms that Indonesian regulation indeed only governs CEX, whereas DEX remains outside the scope of supervision. For the second research question, the conceptual approach enabled an analysis concerning cross-border jurisdictional challenges, the difficulties of off-chain and on-chain evidentiary proof, the pseudonymous nature of blockchain addresses, as well as the technical and institutional impediments in law enforcement. Consequently, the research theory and methods have been able to answer both research questions comprehensively.

However, this research possesses limitations because it did not utilize an empirical approach. The research has not yet examined concrete data from the PPATK (Financial Transaction Reports and Analysis Center), has not elaborated upon blockchain forensic studies in depth, and has not assessed the technical capabilities of law enforcement officials in handling TPPU cases via DEX. Furthermore, technical aspects such as cross-chain laundering mechanisms, smart contract risks, and the governance dynamics of DEX protocols have not been analyzed in greater detail. For subsequent research, a socio-legal approach is required, featuring interviews with regulators, investigators, blockchain

analysts, as well as the collection of empirical data that depicts the actual patterns of DEX misuse in Indonesia. A comparative study with countries such as Singapore, the US, and the European Union is also important for formulating the most suitable regulatory model for Indonesia. With these steps, the development of policies related to digital assets can be more adaptive and effective in facing the risk of money laundering through DEX.

REFERENCES

Bank for International Settlements. *The Crypto Ecosystem : Key Elements and Risks*, 2023.

Bidjuni, Ryan Keynes, Ramdhan Kasim Kasim, and Dince Aisa Kodai. "Penegakan Hukum Terhadap Tindak Pidana Pencucian Uang Melalui Cryptocurrency Di Indonesia." *Gorontalo Justice Research* 1, no. 1 (2025): 208–18.

Dowongi, Anastasya. "Implementasi Hukum Mengenai Tindak Pidana Pencucian Uang (Money Launderyng) Menurut Undang-Undang No 8 Tahun 2010." *Lex Privatum* 13, no. 5 (2024).

FATF. *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Paris: FATF, 2021.

Febriani, Sekar. "Indonesia Peringkat Ke-7 Dunia Untuk Adopsi Kripto, Total Transaksi Sentuh Rp 360 Triliun." Liputan6.com, 2025. https://www.liputan6.com/crypto/read/6201340/indonesia-peringkat-ke-7-dunia-untuk-adopsi-kripto-total-transaksi-sentuh-rp-360-triliun.

Gramedia. "Pengertian Cryptocurrency: Sejarah, Cara Kerja, Jenis, Dan Tujuannya." Gramedia Blog, 2024. https://www.gramedia.com/literasi/cryptocurrency.

Hägele, Sascha. "Centralized Exchanges vs. Decentralized Exchanges in Cryptocurrency Markets: A Systematic Literature Review." *Electronic Markets* 34, no. 1 (2024): 33.

Khairunisa, Amelia, and Atik Winanti. "Batasan Usia Dewasa Dalam Melaksanakan Perkawinan Studi Undang-Undang Nomor 16 Tahun 2019." *JUSTITIA: Jurnal Ilmu Hukum Dan Humaniora* 8, no. 8 (2021): 774–84. http://jurnal.um-tapsel.ac.id/index.php/Justitia%7C.

Limaatmaja, Paskalis Jovena. "Aspek Pidana Terhadap Transaksi Mata Uang Kripto Yang Berpotensi Sebagai Tempat Pencucian Uang" 2, no. 4 (2024): 511–32.

Malamud, Semyon, and Marzena Rostek. "Decentralized Exchange." *American Economic Review* 107, no. 11 (2017): 3320–62.

Marzuki, Peter Mahmud. *Penelitian Hukum: Edisi Revisi*. Prenada Media, 2017.

Monetary Authority of Singapore (MAS). *Payment Services Act 2019*. Singapore: Monetary Authority of Singapore (MAS), 2020. https://www.mas.gov.sg.

Nurhayati, Yati, Ifrani Ifrani, Abdul Halim Barkatullah, and M Yasir Said. "The Issue of

Copyright Infringement in 4.0 Industrial Revolution: Indonesian Case." *Jurnal Media Hukum*, 2019, 122–30.

Oye, Author Emma, Joyce Walker, and Victoria Smith. "The Role of Decentralized Exchanges (DEXs) in Money Laundering Schemes," no. August (2025).

Peraturan BAPPEBTI No. 13 Tahun 2022 Tentang Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (Crypto Asset) Di Bursa Berjangka, n.d.

Peraturan Otoritas Jasa Keuangan Nomor 27 Tahun 2024 Tentang Penyelenggaraan Perdagangan Aset Keuangan Digital Termasuk Aset Kripto, n.d.

Putri, Tiara, Amiludin Amiludin, Dwi Nurfauziah Ahmad, and Hidayatulloh Hidayatulloh. "Inadequate Cryptocurrency and Money Laundering Regulations in Indonesia (Comparative Law of US and Germany)." *Yustisia* 12, no. 2 (2023): 129–52.

Susanto, Asmara Nova, and Wiwik Afifah. "Peran Lembaga Yang Mendukung Penelusuran Alat Bukti Tindak Pidana Pencucian Uang Yang Menggunakan Cryptocurrency." *Media Hukum Indonesia (MHI)* 2, no. 4 (2024).

Tempo. "OJK Sebut Transaksi Kripto Tembus Rp 650 Triliun per Desember 2024, Apa Itu Aset Kripto?" Tempo.co.id, 2024. https://www.tempo.co/ekonomi/ojk-sebut-transaksi-kripto-tembus-rp-650-triliun-per-desember-2024-apa-itu-aset-kripto--1207251 .

Undang-Undang No. 4 Tahun 2023 Tentang Pengembangan Dan Penguatan Sektor Keuangan, 2023.