E-JUSTICE: JOURNAL OF LAW AND TECHNOLOGY

Vol. 1 No. 1, September 2024, pp 16-29

Research Article

Navigating the Crypto Landscape: Exploring the Risks and Potential Misuse of Crypto Assets in Money Laundering

Jefri[1], Saepullah[2]

Corresponding e-mail: jefri.22294031@umkendari.ac.id

Article Information

Article history
Received: May 30th, 2024
Revised: Sept 29th, 2024
Accepted: Sept 29th, 2024

Keywords:
Anonymous; Crypto; Money laundering; Misuse;

How to Cite: Jefri, Jefri and Saepullah, Saepullah. "Navigating the Crypto Landscape: Exploring the Risks and Potential Misuse of Crypto Assets in Money Laundering." *E-Justice: Journal of Law and Technology* 1, no. 1 (2024): 16-29

Abstract

Background: The issue with cryptocurrency lies in its anonymous or pseudo-anonymous characteristics, which create obstacles or difficulties in tracing wealth that is converted into cryptocurrency assets. This results in opportunities for money laundering through cryptocurrency assets.

Methodology: This study is normative research that employs a dual approach, incorporating both legislative analysis and conceptual frameworks to examine the subject matter.

Objectives: This paper aims to address the risks of cryptocurrency asset misuse in money laundering crimes and the potential for committing money laundering through the misuse of cryptocurrency assets.

Findings: Cryptocurrency misuse in money laundering can be identified through mapping threats, vulnerabilities, and impacts, indicating money laundering risks. Money laundering can occur by exploiting cryptocurrency's anonymous characteristics or using nominees in transactions. Additionally, laundering is possible when receiving cryptocurrency accounts containing concealed crime proceeds, provided the receiver knows or suspects the account's criminal origin.

Originality/Novelty: While another research on money laundering focusing on combating the crime, this research introduces the new

[1] Faculty of Law, Universitas Muhammadiyah Kendari, Indonesia | https://orcid.org/0009-0001-1998-8659
[2] Faculty of Law, Universitas Muhammadiyah Kendari, Indonesia | https://orcid.org/0009-0006-3487-9393

potential of money laundering through the utilization the current technology, which is cryptocurrency.

Introduction

Cryptocurrency assets, products of modern technological advancements, have recently garnered significant public attention.[1] This surge in interest has sparked widespread public discourse, particularly following the actions of prominent influencers. These influencers have leveraged their influence to engage in "flexing," encouraging the public to invest in illegal schemes disguised as trading activities, with the influencers acting as affiliates. The wealth accumulated from these illicit activities is subsequently converted into cryptocurrency assets.[2]

In Indonesia, cryptocurrency assets are currently not regarded as currency. This is primarily because cryptocurrencies are not issued by an authorized authority, such as Bank Indonesia. However, in many countries, including the Netherlands, the United Kingdom, Germany, Japan, the United States, and Switzerland, cryptocurrencies are recognized and legitimized as currency. These nations have also implemented policies to prevent their misuse, particularly in money laundering activities.[3]

Cryptocurrency assets are digital assets utilizing blockchain (distributed ledger) and cryptographic technology.[4] These assets are characterized by high price volatility, which prevents them from fulfilling the three functions of money: acting as a store of value, a medium of exchange, and a unit of account. Within the realm of cryptocurrencies, stablecoins have been introduced to protect investment income from this volatility. Legally, cryptocurrency assets are defined as digital commodities that are intangible and whose transaction verification and security do not involve third parties (see Article 1, point 1 of BAPPEBTI Regulation No. 5 of 2019).

[1] Alexey Mikhaylov, "Cryptocurrency Market Analysis from the Open Innovation Perspective," *Journal of Open Innovation: Technology, Market, and Complexity* 6, no. 4 (December 2020): 197, https://doi.org/10.3390/joitmc6040197.
[2] Garcia Krisnando Nathanael, Devi Angeliawati, and Muhadjir Muhadjir, "The Power of Social Media to Influence People In Indonesia: Case Study of Crazy Rich Scam and Big Data of Election Postponement," *JPPI (Jurnal Penelitian Pendidikan Indonesia)* 9, no. 1 (March 9, 2023), https://doi.org/10.29210/020221755.
[3] M. Najibur Rohman, "Tinjauan Yuridis Normatif Terhadap Regulasi Mata Uang Kripto (Crypto Currency) Di Indonesia," *Jurnal Supremasi*, August 31, 2021, 1–10, https://doi.org/10.35457/supremasi.v11i2.1284.
[4] Shabrina Puspasari, "Perlindungan Hukum Bagi Investor Pada Transaksi Aset Kripto Dalam Bursa Berjangka Komoditi," *Jurist-Diction* 3, no. 1 (January 29, 2020): 303, https://doi.org/10.20473/jd.v3i1.17638.

Currently, in Indonesia, there is a significant risk of using cryptocurrency assets as instruments for money laundering. This concern is substantiated by emerging cases of illegal investments, where perpetrators are also charged with money laundering, allegedly using cryptocurrency to conceal their illicit gains. Despite this, law enforcement agencies have not yet fully focused on addressing the use of cryptocurrency in money laundering activities. Therefore, raising public awareness about the risks of money laundering involving cryptocurrency assets is essential.

Currently, the cryptocurrency trading industry in Indonesia is emerging as a new financial institution. This status presents opportunities for criminals to misuse it as an instrument for money laundering. According to the Sectoral Risk Assessment of cryptocurrency trading in Indonesia, conducted by PPATK in collaboration with BAPPEBTI and the Ministry of Trade, it is noted that entrepreneurs and politically exposed persons (PEPs) are customer profiles at very high risk of engaging in money laundering activities. Additionally, Bitcoin is identified as a high-risk product and service for use in money laundering within the cryptocurrency trading sector. This aligns with the recent case of an influencer accused of illegal binary option investments and money laundering, whose profile matches that of an entrepreneur and who allegedly used Bitcoin in these crimes.[5]

Given these events, it is evident that the use of cryptocurrency assets for money laundering is no longer merely a risk but has become an actual occurrence, known in criminal law as a criminal act (*strafbaar feit*). Therefore, it is necessary to review and examine the potential forms of money laundering crimes that can be committed using cryptocurrency assets.

Based on the previously discussed points, the author has formulated the title of this paper as "Risks and Possibilities of Cryptocurrency Asset Misuse in Money Laundering Crimes." This title reflects the issues identified in this study: What are the risks of cryptocurrency asset misuse in money laundering crimes? And what are the possibilities of money laundering crimes occurring through the misuse of cryptocurrency assets?

Research Method

This paper employs a normative research method, as all legal research should fundamentally be normative. The distinguishing factor lies in the legal materials and approaches used. This study adopts the following approaches: **Conceptual Approach:** This approach is based on legal doctrines and theoretical perspectives in the field of law. In this paper, concepts and theories related to cryptocurrency assets and money laundering offenses serve as the conceptual foundation for analyzing and addressing the issues raised. **Statutory Approach:** This approach involves examining all relevant legislation related to

[5] Dewanti Arya Maha Rani, I Nyoman Gede Sugiartha, and Ni Made Sukaryati Karma, "Uang Virtual (Cryptocurrency) Sebagai Sarana Tindak Pidana Pencucian Uang Dalam Perdagangan Saham," *Jurnal Konstruksi Hukum* 2, no. 1 (March 1, 2021): 19–23, https://doi.org/10.22225/jkh.2.1.2961.19-23.

the legal issues analyzed. Specifically, this paper analyzes the Money Laundering Act, Ministry of Trade Regulation No. 99 of 2018, and BAPPEBTI Regulation No. 5 of 2019.

Cryptocurrency Abuse and Money Laundering: A Growing Threat

Risk is a concept that reflects uncertainty or the potential occurrence of adverse or harmful outcomes. Therefore, it is essential to take accurate and targeted measures to prevent these negative consequences. By doing so, any practices that could result in losses can be anticipated early, mitigating the risk of such losses. However, before these measures can be implemented, it is crucial to first assess the risk to enable effective control.[6]

Nearly all crimes are triggered by certain circumstances or actions. In the context of money laundering, perpetrators typically engage in such criminal activities because they aim to enjoy the proceeds of their illegal acts calmly and make it difficult for their wealth to be detected or traced. This is because the acquired wealth appears to originate from legitimate sources. Neil Jensen concurs, stating that money laundering involves the transformation of profits from illegal activities into wealth that appears to be obtained from legal or legitimate origins.[7]

Money laundering is defined as a series of activities carried out by an individual or a group of individuals involving proceeds from criminal activities. The intention is to obscure the origins of the illicit gains, making them difficult to trace or appear as if they are legitimate assets, using various methods. Therefore, as a new and modern financial system operated in digital form, it is plausible that cryptocurrency assets could be utilized as tools to facilitate money laundering crimes.[8]

In international guidelines concerning the calculation of AML (Anti-Money Laundering) and CFT (Counter Financing of Terrorism) risks issued by the International Monetary Fund (IMF), it is explained that "risk can be expressed by the equation: R = f[(T),(V)] x C", where T represents threat, V represents vulnerability, and C represents consequence. Threat refers to entities, objects, or criminal activities that have the potential to cause harm, which in the context of money laundering crimes may include perpetrators and the source of funds. Vulnerability refers to issues that can be exploited by criminals in perpetrating their crimes, which in the context of money laundering can be identified in weaknesses within the system, including regulations, services, and products that can be exploited by criminals in laundering money. Consequence refers to the impact generated by criminals and their crimes, both on the financial system and industry, as well as on the broader socio-economic

[6] Eko Sudarmanto, "Manajemen Risiko: Deteksi Dini Upaya Pencegahan Fraud," *Jurnal Ilmu Manajemen* 9, no. 2 (June 15, 2020): 107, https://doi.org/10.32502/jimn.v9i2.2506.
[7] Georgy Rusanov and Yury Pudovochkin, "Money Laundering in the Modern Crime System," *Journal of Money Laundering Control* 24, no. 4 (October 21, 2021): 860–68, https://doi.org/10.1108/JMLC-08-2020-0085.
[8] Christoph Wronka, "'Cyber-Laundering': The Change of Money Laundering in the Digital Age," *Journal of Money Laundering Control* 25, no. 2 (April 21, 2022): 330–44, https://doi.org/10.1108/JMLC-04-2021-0035.

conditions of society. Therefore, the following analysis will be presented regarding these aspects.

Threat

In identifying the threat of risk associated with cryptocurrency asset misuse for money laundering, it is essential to consider who is prone to engaging in activities that serve as the source of funds. The Financial Action Task Force (FATF) underscores the significance of examining the users of services and businesses involved in these activities, which contribute to the acquisition of assets from service users. In the cryptocurrency trading sector in Indonesia, the sectoral risk assessment highlights that individuals classified as Entrepreneurs and Politically Exposed Persons (PEPs) pose a high risk of involvement in money laundering activities. Furthermore, concerning the origin of assets from service users, predicate crimes such as Narcotics, Psychotropics, and Corruption are identified as posing a significant risk in the misuse of cryptocurrency assets for money laundering purposes.

Understanding these dynamics is crucial for devising effective strategies to mitigate the risk of cryptocurrency asset misuse in money laundering schemes. By targeting high-risk individuals and predicate crimes, authorities can better safeguard the integrity of financial systems and prevent illicit activities facilitated by cryptocurrency transactions.

Vulnerability

Cryptocurrency assets represent a new form of commodity that has experienced rapid advancement and development, particularly since the emergence of Bitcoin in 2009, and continues to evolve. This dynamic market saw the introduction of cryptocurrency trading in Indonesia in 2014. In 2018, the Ministry of Trade issued Regulation No. 99 of 2018 concerning the General Policy for the Implementation of Cryptocurrency Futures Trading, while in 2019, BAPPEBTI (Indonesia's Commodity Futures Trading Regulatory Agency) issued Regulation No. 5 of 2019 regarding the Technical Provisions for the Implementation of Physical Market for Cryptocurrency Assets on Futures Exchanges. These regulatory measures reflect the efforts to establish a framework for the trading and oversight of cryptocurrency assets within Indonesia, marking significant milestones in the country's engagement with this rapidly evolving financial sector.

One factor that renders cryptocurrency assets susceptible to misuse is the heightened anonymity and increased barriers to detection by law enforcement agencies regarding criminal activities conducted through cryptocurrency transactions. These factors serve as an attraction for criminals seeking to conceal or launder illicitly obtained funds. Moreover, criminals can transfer cryptocurrency assets operating on transparent public blockchains, such as Bitcoin, to cryptocurrency exchanges or online trading platforms and swiftly trade them for anonymity-enhanced cryptocurrencies (AEC) or privacy coins. This ability to obfuscate transaction trails and conceal the identities of those involved further complicates

efforts to track and investigate illicit financial activities conducted using cryptocurrency assets.

In general, cryptocurrency assets like Bitcoin are considered anonymous forms of internet currency. However, Bitcoin and most other virtual assets, although not fully anonymous, often operate under the guise of pseudonymity. Pseudonymity is defined as "traceable anonymity," meaning transactions can still be tracked using technical procedures to associate individuals (service users). However, in general transaction tracking, the identities of users remain undisclosed. The difficulty or barrier associated with tracing the true owners of funds in a cryptocurrency account projects that the existence of cryptocurrency assets provides an opportunity for criminals to secure their assets there. This scenario represents a vulnerability in the misuse of cryptocurrency assets to conceal or launder proceeds from criminal activities.[9]

In light of the anonymous or pseudo-anonymous nature of cryptocurrency assets, it is important to note that strong privacy protections are often built into transactions, such as those involving Bitcoin. During these transactions, the system does not reveal the identities of the parties involved. Furthermore, Bitcoin users can only be traced using numerical codes, which are frequently transferred using various pseudonyms.[10]

The explanations provided above highlight the vulnerability of cryptocurrency asset misuse due to their anonymous or pseudo-anonymous nature, which poses a risk for exploitation by criminals to make their illicit gains difficult to trace. The difficulty in tracing these illicit assets underscores the "intent to conceal criminal proceeds," which is the essence of money laundering.[11]

In a research study, it was noted that one vulnerability in the legal system regarding the misuse of cryptocurrency assets for money laundering purposes is the lack of provisions regarding the application of the "know your customer" (KYC) principle.[12] In Indonesia, efforts have been made to mitigate this risk. One critical mitigation effort is outlined in BAPPEBTI Regulation No. 5 of 2019, which specifies requirements for prospective physical cryptocurrency traders to implement an AML/CFT (Anti-Money Laundering/Combating the Financing of Terrorism) program prescribed by BAPPEBTI.

---

[9] Alicia Schmidt, "Virtual Assets: Compelling a New Anti-Money Laundering and Counter-Terrorism Financing Regulatory Model," *International Journal of Law and Information Technology* 29, no. 4 (March 12, 2022): 332–63, https://doi.org/10.1093/ijlit/eaac001.

[10] Dewi Asri Puanandini, "Pidana Pencucian Uang Hasil Kejahatan Siber (Cyber Crime) Melalui Mata Uang Digital (Crypto Currency)," *JURNAL PEMULIAAN HUKUM* 4, no. 2 (October 30, 2021): 57–70, https://doi.org/10.30999/jph.v4i2.1480.

[11] Ali Geno, "Tindak Pidana Kejahatan Pencucian Uang (Money Laundering) Dalam Pandangan KUHP Dan Hukum Pidana Islam," *TAWAZUN : Journal of Sharia Economic Law* 2, no. 1 (June 23, 2019): 1, https://doi.org/10.21043/tawazun.v2i1.5223.

[12] Puanandini, "Pidana Pencucian Uang Hasil Kejahatan Siber (Cyber Crime) Melalui Mata Uang Digital (Crypto Currency)."

These requirements include obtaining approval to facilitate customer transactions in the physical cryptocurrency market, engaging in cryptocurrency trading, using customer cryptocurrency accounts, and operating trading activities during the registration period. One component of the AML/CFT program is the obligation for financial institutions to apply the KYC principle. Therefore, concerning the risk vulnerability issue stemming from the lack of regulation regarding the implementation of the KYC principle in Indonesia, this has been addressed through the issuance of BAPPEBTI Regulation No. 5 of 2019.

Impact

Money laundering poses a significant threat to global economic prosperity, undermining the integrity of financial systems and funding further criminal activities that impact the safety and well-being of society.[13] There are numerous methods criminals employ for money laundering, including utilizing modern financial products and technologies. Over the past two decades, there has been a global increase in money laundering practices since its criminalization. In the pursuit of money laundering, prospective traditional customers tend to avoid using regular banking services and instead turn to decentralized financial systems as an alternative solution.[14] One form of decentralized financial system is cryptocurrency assets. Cryptocurrency assets consist of decentralized cryptographic codes that can be stored digitally and transferred like electronic mail. Additionally, cryptocurrency assets can serve as a means of payment, although their recognition as currency is lacking in Indonesia.[15]

The popularity of cryptocurrency assets has grown since Bitcoin gained status as a required payment method on the Silk Road dark web market, where virtual assets are often associated. The dark web is commonly used to provide anonymity for individuals seeking to conceal private information, often by those engaged in illegal activities. Despite its unstructured design, the anonymity it offers remains appealing to criminals looking to hide the proceeds of their crimes. Consequently, the dark web has facilitated the control of criminal activities and has proven to be a challenge for law enforcement efforts. [16]

Consequences, in risk assessment, are interpreted as the repercussions arising from the potential occurrence of money laundering crimes in cryptocurrency trading. The impact of

[13] Kishore Singh and Peter Best, "Anti-Money Laundering: Using Data Visualization to Identify Suspicious Activity," *International Journal of Accounting Information Systems* 34 (September 2019): 100418, https://doi.org/10.1016/j.accinf.2019.06.001.
[14] Ayodeji Aluko and Mahmood Bagheri, "The Impact of Money Laundering on Economic and Financial Stability and on Political Development in Developing Countries," *Journal of Money Laundering Control* 15, no. 4 (October 5, 2012): 442–57, https://doi.org/10.1108/13685201211266024.
[15] Aditya Rafi Fauzan and Rianda Dirkareshza, "Lex Crypto: Perbandingan Landasan Hukum Terhadap Dampak Keberadaan Bitcoin Antara Indonesia Dengan El Salvador," *Pandecta Research Law Journal* 16, no. 2 (2021): 320–35, https://doi.org/https://doi.org/10.15294/pandecta.v16i2.31838.
[16] Sesha Kethineni and Ying Cao, "The Rise in Popularity of Cryptocurrency and Associated Criminal Activity," *International Criminal Justice Review* 30, no. 3 (September 6, 2020): 325–44, https://doi.org/10.1177/1057567719827051.

cryptocurrency assets is often derived from transaction value data. As of 2020 alone, the value of cryptocurrency assets received by the dark web market has shown remarkably significant results, amounting to USD 1.7 billion.[17]

In many respects, the dark web serves as a one-stop shop for modern crime. With numerous examples of crimes offering payment in cryptocurrency assets and the profits from these crimes utilizing available anonymous mixing services on the dark web to obscure transaction flows, or simply requesting payment in cryptocurrency to enhance transaction anonymity. To facilitate transactions, the dark web provides users with the convenience to circumvent various anti-money laundering regulations, such as providing a marketplace for stolen identities, to deceive the requirements of the KYC principle. With the occurrence of money laundering crimes abusing various financial systems, including cryptocurrency assets, to conceal or disguise the origin of criminal proceeds obtained by criminals, this can further have negative effects on society, especially in the economic sector.[18]

From the explanation above, it is evident that one of the main weaknesses in combating the impact of modern and renewable technologies (such as cryptocurrency assets) in money laundering crimes is the inadequacy of technology systems in detecting the flow of illegal funds. Therefore, an effective technological solution is a crucial element in avoiding the risks associated with money laundering impacts.[19]

Money Laundering Potential through Crypto Assets

Legally, in Indonesia, money laundering encompasses all actions that meet the elements of a criminal offense as stipulated in the Anti-Money Laundering Law (UU TPPU), specifically outlined in Article 1, point 1. The criminalization of money laundering is articulated in Articles 3, 4, and 5 (for natural persons) and Article 6, paragraph 2 (for legal entities), along with other provisions related to associated crimes in Articles 11 to 16 of the UU TPPU.

According to Teichmann, money laundering involves any act aimed at thwarting the identification, tracing, or seizure of assets known or suspected to originate from criminal activities.[20] Korejo, et al., define money laundering as the process of converting illicit assets obtained through criminal means and mixing them with legitimate funds to make them appear lawful, thereby making it challenging to distinguish between legal and illegal

[17] Schmidt, "Virtual Assets: Compelling a New Anti-Money Laundering and Counter-Terrorism Financing Regulatory Model."
[18] Iwan Kurniawan, "Perkembangan Tindak Pidana Pencucian Uang (Money Laundering) Dan Dampaknya Terhadap Sektor Ekonomi Dan Bisnis," *Jurnal Ilmu Hukum* 4, no. 1 (March 8, 2013), https://doi.org/10.30652/jih.v3i1.1037.
[19] Singh and Best, "Anti-Money Laundering: Using Data Visualization to Identify Suspicious Activity."
[20] Fabian Maximilian Johannes Teichmann, "Twelve Methods of Money Laundering," *Journal of Money Laundering Control* 20, no. 2 (May 2, 2017): 130–37, https://doi.org/10.1108/JMLC-05-2016-0018.

money.[21] From these doctrinal perspectives, money laundering can be understood as actions undertaken to (a) obstruct or complicate the identification, tracing, or seizure of illicit wealth (concealment), or (b) make the proceeds of crime appear as legitimate assets (disguise). Thus, the essence of money laundering is the effort to obscure or mask the origins of criminal proceeds.

In the analysis of money laundering, typology analysis serves as an instrument to examine the modus operandi employed by criminals. One common modus operandi or typology in money laundering is the use of anonymous asset types. A concrete example of such anonymous assets is the use of cash (cash withdrawals and deposits). However, this can also include electronic payment systems and financial systems, such as personal accounts with anonymous numbers.

These explanations illustrate that one typology or modus operandi used by money launderers to conceal or disguise the proceeds of their crimes involves utilizing various financial products with anonymous characteristics. This aligns with the nature of crypto assets, which also possess anonymous attributes. According to the FATF report to the G-20, the primary money laundering risk associated with crypto assets is their anonymity. Many crypto assets have public, permissionless, and decentralized ledgers. While transaction ledgers are publicly accessible, they often do not include user identity information. Additionally, there may be no central administrator monitoring transactions. Crypto assets are also private, allowing only a limited group of entities to initiate transactions or view and verify the ledger.[22] Some crypto assets, known as privacy coins or anonymity-enhanced cryptocurrencies, employ additional cryptographic software to further obscure transactions. This inherent anonymity can make crypto asset transactions difficult to monitor adequately, enabling illicit activities to occur beyond regulatory boundaries, and allowing organized criminals to access "clean money" with ease.[23]

At least two characteristics of coins in crypto assets—anonymous and pseudo-anonymous—are detailed in the following table:

Table 1. Types and Characteristic of Crypto Assets

No.	Types of crypto assets	Coin Characteristic
1.	Bitcoin (BTC)	Pseudo Anonymous

[21] Muhammad Saleem Korejo, Ramalinggam Rajamanickam, and Muhamad Helmi Md. Said, "The Concept of Money Laundering: A Quest for Legal Definition," *Journal of Money Laundering Control* 24, no. 4 (October 21, 2021): 725–36, https://doi.org/10.1108/JMLC-05-2020-0045.

[22] Sheng-Feng Hsieh and Gerard Brennan, "Issues, Risks, and Challenges for Auditing Crypto Asset Transactions," *International Journal of Accounting Information Systems* 46 (September 2022): 100569, https://doi.org/10.1016/j.accinf.2022.100569.

[23] Eray Arda Akartuna, Shane D. Johnson, and Amy E. Thornton, "The Money Laundering and Terrorist Financing Risks of New and Disruptive Technologies: A Futures-Oriented Scoping Review," *Security Journal* 36, no. 4 (December 19, 2023): 615–50, https://doi.org/10.1057/s41284-022-00356-z.

2.	Ethereum (ETH)	Pseudo Anonymous
3.	Ripple (XRP)	Pseudo Anonymous
4.	Bitcoin Cash (BCH)	Pseudo Anonymous
5.	Litecoin (LTC)	Pseudo Anonymous
6.	Stellar (XLM)	Pseudo Anonymous
7.	Cardano (ADA)	Pseudo Anonymous
8.	IOTA (MIOTA)	Pseudo Anonymous
9.	NEO (NEO)	Pseudo Anonymous
10.	Monero (XMR)	Anonymous
11.	Dash (DASH)	Anonymous

An anonymous asset is one that is inherently untraceable or extremely difficult to trace. Conversely, pseudonymity represents 'traceable anonymity,' wherein it is feasible to associate transactions with individuals (service users) through technical procedures. However, during a general transaction trace, the user's true identity remains undiscovered. These characteristics create significant obstacles or difficulties in determining the actual owner of funds within a cryptocurrency account.

The above explanation further illustrates that the characteristics of anonymity or at least pseudonymity inherent in crypto assets provide opportunities for misuse by criminals seeking to conceal or disguise the proceeds of their illicit activities. However, asserting that a particular typology represents money laundering should not be based solely on a single factor. Instead, it requires an analysis that combines this typology with the legal facts surrounding the transactions, ultimately resulting in a state where the assets are hidden or disguised. This approach concretely reflects the element of 'with the intent to conceal or disguise the origin of illicit proceeds.'

In simple terms, it is not the mere alignment between the typology and the criminal's actions that defines the act of money laundering. Instead, it is the actual concealment or disguising of the proceeds of crime that results from the alignment of the criminal's actions with the typology that constitutes money laundering. More specifically, when contextualized with the misuse of crypto assets for the purpose of concealing or disguising the proceeds of crime, it is not the mere alignment between the typology of the use of anonymous asset types and the criminal's action of depositing illicit gains into crypto assets that establishes money laundering. Rather, it is the fact that this alignment results in the proceeds becoming difficult to trace or identify, which concretely represents the disguised nature of the illicit gains deposited into the crypto assets.

Based on the analysis, it is possible to question why the proceeds of a crime must be considered concealed or disguised to establish the occurrence of money laundering, especially when the element of the offense is stated as 'with the intent to conceal or disguise

the origin of the proceeds of crime.' The explanation for this lies in the phrase 'with the intent,' which indicates that both the action and its consequences are known and intended by the perpetrator. This means that the focus is not solely on the act of concealing or disguising but also on the outcome of these actions. Consequently, the outcome of the act of concealing or disguising the proceeds of crime, which is known and intended by the perpetrator, is that the illicit gains are indeed concealed or disguised.

In addition to the modus operandi or typology of using anonymous asset types, which criminals might exploit to launder money through crypto assets, there is also the possibility of employing the use of nominee or strawman typology. The use of a nominee or strawman involves using another person's identity or instructing someone else to carry out transactions (e.g., deposits or withdrawals) with the intention that, even if law enforcement traces the transaction, it would be difficult to establish a connection between the criminal and the other party. This typology allows the criminal to open a crypto asset account under another person's identity and then deposit the illicit proceeds into that account.

Consequently, even if there is intensive tracing to identify the account owner, the identity that appears in the transactions is only that of the 'other party.' However, the actual beneficiary owner of the transaction is the criminal who used the other person's identity to open the crypto account. This creates significant obstacles and complexities in tracing the proceeds of crime obtained by the criminal, effectively fulfilling the element of 'with the intent to conceal the proceeds of crime.'

Additionally, another scenario arises where a criminal, having already concealed or disguised the proceeds of their crime within a crypto account, subsequently transfers that account to another party. If it can be proven that the recipient knew or had reasonable grounds to suspect that the crypto account contained illicit funds, they can also be prosecuted for money laundering as a 'passive money laundering offender.' Passive money laundering, as defined under Article 5, paragraph (1) of the Indonesian Money Laundering Law (UU TPPU), criminalizes individuals who knowingly receive or hold assets derived from criminal activities.[24]

Conclusion

The risk of crypto asset misuse in money laundering is identifiable by mapping three variables: threats, vulnerabilities, and impact. Threats stem from parties and predicate offenses ripe for exploitation in money laundering schemes involving crypto assets. Vulnerabilities arise from regulatory gaps and weaknesses in crypto asset products, which criminals exploit to launder money. Meanwhile, the impact manifests in the consequences for the financial system resulting from money laundering offenses facilitated through crypto asset misuse. Exploitation often occurs due to the anonymous or pseudo-

[24] Muh. Afdal Yanuar, "Posibilitas Eksistensi Jenis Tindak Pidana Pencucian Uang Stand Alone Money Laundering Di Indonesia," *Nagari Law Review* 5, no. 1 (October 31, 2021): 23, https://doi.org/10.25077/nalrev.v.5.i.1.p.23-40.2021.

anonymous nature of certain coins, aligning with typologies like using anonymous asset types. This misuse can involve crypto accounts held by nominees or strawmen, with illicit proceeds deposited into these accounts. Additionally, third parties may receive hidden or disguised illicit proceeds in crypto accounts, knowing or suspecting their criminal origins. To address this, authorities should collaborate with crypto asset traders to develop tracking systems for crypto transactions, especially those with fully anonymous characteristics, aiding law enforcement in combating money laundering and other economic crimes. Moreover, enhancing the knowledge and awareness of law enforcement and relevant stakeholders regarding crypto asset characteristics and transaction patterns is crucial for detecting and preventing crypto asset misuse for money laundering.

Acknowledgment

None.

Conflict of Interest

There are no relevant financial or non-financial competing interests to report.

Author(s) Contribution

Author 1: initiated the research ideas, instrument construction, data collection, analysis, and draft writing; **Author 2:** revised the research ideas, literature review, data presentation and analysis, and the final draft.

References

Akartuna, Eray Arda, Shane D. Johnson, and Amy E. Thornton. "The Money Laundering and Terrorist Financing Risks of New and Disruptive Technologies: A Futures-Oriented Scoping Review." *Security Journal* 36, no. 4 (December 19, 2023): 615–50. https://doi.org/10.1057/s41284-022-00356-z.

Aluko, Ayodeji, and Mahmood Bagheri. "The Impact of Money Laundering on Economic and Financial Stability and on Political Development in Developing Countries." *Journal of Money Laundering Control* 15, no. 4 (October 5, 2012): 442–57. https://doi.org/10.1108/13685201211266024.

Fauzan, Aditya Rafi, and Rianda Dirkareshza. "Lex Crypto: Perbandingan Landasan Hukum Terhadap Dampak Keberadaan Bitcoin Antara Indonesia Dengan El Salvador." *Pandecta Research Law Journal* 16, no. 2 (2021): 320–35. https://doi.org/https://doi.org/10.15294/pandecta.v16i2.31838.

Geno, Ali. "Tindak Pidana Kejahatan Pencucian Uang (Money Laundering) Dalam Pandangan KUHP Dan Hukum Pidana Islam." *TAWAZUN : Journal of Sharia Economic Law* 2, no. 1 (June 23, 2019): 1. https://doi.org/10.21043/tawazun.v2i1.5223.

Hsieh, Sheng-Feng, and Gerard Brennan. "Issues, Risks, and Challenges for Auditing Crypto

Asset Transactions." *International Journal of Accounting Information Systems* 46 (September 2022): 100569. https://doi.org/10.1016/j.accinf.2022.100569.

Kethineni, Sesha, and Ying Cao. "The Rise in Popularity of Cryptocurrency and Associated Criminal Activity." *International Criminal Justice Review* 30, no. 3 (September 6, 2020): 325–44. https://doi.org/10.1177/1057567719827051.

Korejo, Muhammad Saleem, Ramalinggam Rajamanickam, and Muhamad Helmi Md. Said. "The Concept of Money Laundering: A Quest for Legal Definition." *Journal of Money Laundering Control* 24, no. 4 (October 21, 2021): 725–36. https://doi.org/10.1108/JMLC-05-2020-0045.

Kurniawan, Iwan. "Perkembangan Tindak Pidana Pencucian Uang (Money Laundering) Dan Dampaknya Terhadap Sektor Ekonomi Dan Bisnis." *Jurnal Ilmu Hukum* 4, no. 1 (March 8, 2013). https://doi.org/10.30652/jih.v3i1.1037.

Maha Rani, Dewanti Arya, I Nyoman Gede Sugiartha, and Ni Made Sukaryati Karma. "Uang Virtual (Cryptocurrency) Sebagai Sarana Tindak Pidana Pencucian Uang Dalam Perdagangan Saham." *Jurnal Konstruksi Hukum* 2, no. 1 (March 1, 2021): 19–23. https://doi.org/10.22225/jkh.2.1.2961.19-23.

Mikhaylov, Alexey. "Cryptocurrency Market Analysis from the Open Innovation Perspective." *Journal of Open Innovation: Technology, Market, and Complexity* 6, no. 4 (December 2020): 197. https://doi.org/10.3390/joitmc6040197.

Nathanael, Garcia Krisnando, Devi Angeliawati, and Muhadjir Muhadjir. "The Power of Social Media to Influence People In Indonesia: Case Study of Crazy Rich Scam and Big Data of Election Postponement." *JPPI (Jurnal Penelitian Pendidikan Indonesia)* 9, no. 1 (March 9, 2023). https://doi.org/10.29210/020221755.

Puanandini, Dewi Asri. "Pidana Pencucian Uang Hasil Kejahatan Siber (Cyber Crime) Melalui Mata Uang Digital (Crypto Currency)." *JURNAL PEMULIAAN HUKUM* 4, no. 2 (October 30, 2021): 57–70. https://doi.org/10.30999/jph.v4i2.1480.

Puspasari, Shabrina. "Perlindungan Hukum Bagi Investor Pada Transaksi Aset Kripto Dalam Bursa Berjangka Komoditi." *Jurist-Diction* 3, no. 1 (January 29, 2020): 303. https://doi.org/10.20473/jd.v3i1.17638.

Rohman, M. Najibur. "Tinjauan Yuridis Normatif Terhadap Regulasi Mata Uang Kripto (Crypto Currency) Di Indonesia." *Jurnal Supremasi*, August 31, 2021, 1–10. https://doi.org/10.35457/supremasi.v11i2.1284.

Rusanov, Georgy, and Yury Pudovochkin. "Money Laundering in the Modern Crime System." *Journal of Money Laundering Control* 24, no. 4 (October 21, 2021): 860–68. https://doi.org/10.1108/JMLC-08-2020-0085.

Schmidt, Alicia. "Virtual Assets: Compelling a New Anti-Money Laundering and Counter-Terrorism Financing Regulatory Model." *International Journal of Law and Information*

Technology 29, no. 4 (March 12, 2022): 332–63. https://doi.org/10.1093/ijlit/eaac001.

Singh, Kishore, and Peter Best. "Anti-Money Laundering: Using Data Visualization to Identify Suspicious Activity." *International Journal of Accounting Information Systems* 34 (September 2019): 100418. https://doi.org/10.1016/j.accinf.2019.06.001.

Sudarmanto, Eko. "Manajemen Risiko: Deteksi Dini Upaya Pencegahan Fraud." *Jurnal Ilmu Manajemen* 9, no. 2 (June 15, 2020): 107. https://doi.org/10.32502/jimn.v9i2.2506.

Teichmann, Fabian Maximilian Johannes. "Twelve Methods of Money Laundering." *Journal of Money Laundering Control* 20, no. 2 (May 2, 2017): 130–37. https://doi.org/10.1108/JMLC-05-2016-0018.

Wronka, Christoph. "'Cyber-Laundering': The Change of Money Laundering in the Digital Age." *Journal of Money Laundering Control* 25, no. 2 (April 21, 2022): 330–44. https://doi.org/10.1108/JMLC-04-2021-0035.

Yanuar, Muh. Afdal. "Posibilitas Eksistensi Jenis Tindak Pidana Pencucian Uang Stand Alone Money Laundering Di Indonesia." *Nagari Law Review* 5, no. 1 (October 31, 2021): 23. https://doi.org/10.25077/nalrev.v.5.i.1.p.23-40.2021.