



Trends and Prevention of Cryptocurrency-Based Money Laundering Crimes

Mohammad Nur Bobby Putra Yusra^{1*}, Arthur Josias Simon Runturambi², Bondan Widiawan³

^{1,2,3}SKSG Universitas Indonesia, Depok, DKI Jakarta, Indonesia

E-mail: bobbyputrayusra@gmail.com^{1*}, a.josias@ui.ac.id², widiawanbondan@gmail.com³

ABSTRACT

In Indonesia, Cryptocurrency, on the one hand, is not recognized as a legal tender, so it does not have a legal umbrella, and the risk of its use is borne by the user himself. On the other hand, cryptocurrencies are included in the list of commodities that can be used as the subject of Futures Contracts traded on the Futures Exchange because, from their use, it is expected to make a positive contribution to futures trading in Indonesia. These two contradictory things of cryptocurrency regulation are then faced with a phenomenon called cryptocurrency-based TPPU. This study uses a descriptive method combined with a qualitative approach. The data in this study is primary data sourced from the results of interviews and data from the Metro Jaya Police, and the secondary data used to support the research is literature in the form of books, research journals and online scientific journal data. The data that has been collected is analyzed by data reduction methods and triangulation techniques. The location of the research is the Metro Jaya Police and the University of Indonesia Library. From this study, it is known that in Indonesia, there are no special rules governing this cryptocurrency-based anti-corruption, and there has been no cooperation between law enforcement for its prevention.

Keywords: Money Laundering, Cryptocurrency, Crimes.

INTRODUCTION

The use of cryptocurrencies, which is currently increasing rapidly, has brought a significant impact on the global financial landscape (Azarenkova et al., 2018; Jacobs, 2018; Rejeb et al., 2021). Bitcoin, Ethereum, Altcoin, and various other types of cryptocurrencies, have attracted the interest of market participants, investors, and business actors around the world, including in Indonesia, because of their unique characteristics, such as being present in digital form, applicable equally in every country, encrypted, decentralized, and many more.

However, the sustainability and popularity of cryptocurrencies also bring new challenges related to financial security and public order (Fadeyi et al., 2019; Giungato et al., 2017; Kethineni

& Cao, 2020; Vaz & Brown, 2020). One main issue that needs to be mitigated is the risk of cryptocurrency-based Money Laundering Crimes (hereinafter abbreviated as TPPU).

As is well known, currently the practice of TPPU has penetrated various aspects along with the development of technology. Perpetrators of TPPU can easily access advanced technology and store or send the proceeds of the original crime to various platforms, including cryptocurrencies.

Cryptocurrencies' characteristics, such as relative anonymity and decentralization, create opportunities for TPPU perpetrators to operate in the shadows, avoiding effective detection. This factor is further complicated by the fact that cryptocurrency users can have more than one account and execute transactions in different places and times simultaneously and without constraints.

The 2023 Directorate of Criminal Investigation report of the Metro Jaya Police, as shown in the image above, shows that the number of cryptocurrency-based TPPU cases on wealth resulting from online fraud, hacking, ransomware and malware occurred throughout 2023. Based on the data presented, there are 40 police reports related to cryptocurrency-based crimes with an estimated loss of Rp.200,000,000 (two hundred million Rupiah) per case, which, if accumulated in total, amounts to Rp.8,000,000,000 (eight billion Rupiah).

An example of a cryptocurrency-based TPPU case that occurred was the server break-in of one of the payment system infrastructure providers, PT. ALTO Network. After that, funds in the form of cryptocurrency were transferred to 391 accounts with a total money turnover of Rp.24,500,000,000 (twenty-four billion five hundred million Rupiah). Unfortunately, the case has not yet found a bright spot.

The characteristics of cryptocurrencies are juxtaposed with the equally unique character of TPPU, shaping it into a complex cybercrime (Borghetti & Katos, 2021). This poses a challenge for law enforcement to identify the perpetrators, trace the transactions involved, and gather sufficient evidence. Therefore, the author is interested in examining the impact and prevention of cryptocurrency-based anti-trafficking in this paper.

The topic of cryptocurrency-based TPPU in Indonesia has been studied by several authors or researchers, one of which is in a journal entitled "Cryptocurrency Legal Regulation and Prevention of Its Misuse in Indonesia" by Murti et al. (2024), which discusses cryptocurrencies in general and focuses on legal regulations in Indonesia if there is abuse. In this paper, the author looks at the perspective of law enforcement, which discusses the trend of cryptocurrency-based anti-corruption and its prevention efforts from the author's side as a law enforcer.

RESEARCH METHODS

This study uses a descriptive method combined with a qualitative approach (Kim et al., 2017; Taguchi, 2018). The data in this study is primary data sourced from the results of interviews and data from the Metro Jaya Police, and the secondary data used to support the research is

literature in the form of books, research journals and online scientific journal data. The data that has been collected is analyzed using data reduction methods and triangulation techniques (Flick, 2018; Leech & Onwuegbuzie, 2007; Namey et al., 2008). The location of the research is the Metro Jaya Police and the University of Indonesia Library.

RESULTS AND DISCUSSION

Cryptocurrency-Based TPPU

Cryptocurrencies have succeeded in changing people's views of the long-standing monetary and financial system by eliminating trust in third parties in transactions and replacing these third parties with proofs or cryptographic systems. Thus, authorization by third parties such as banks or the state is no longer needed (decentralized). This aims to maintain the security and confidentiality of the data of parties who transact crypto.

On the one hand, the characteristics of this cryptocurrency are an advantage for its users, but on the other hand, it creates a gap in the occurrence of TPPU. As explained earlier, TPPU is not a single criminal act but a follow-up criminal act (hidden or disguised wealth is the result of the original criminal act). In the context of TPPU, the confidentiality of data and the decentralization that is favored by cryptocurrencies can be used as a means to hide or disguise the origin, source, location, designation, transfer of rights, or actual ownership of wealth that it knows or should suspect is the result of the original criminal act.

Divina (2021) the following are the stages of cryptocurrency-based TPPU with the example of Bitcoin:

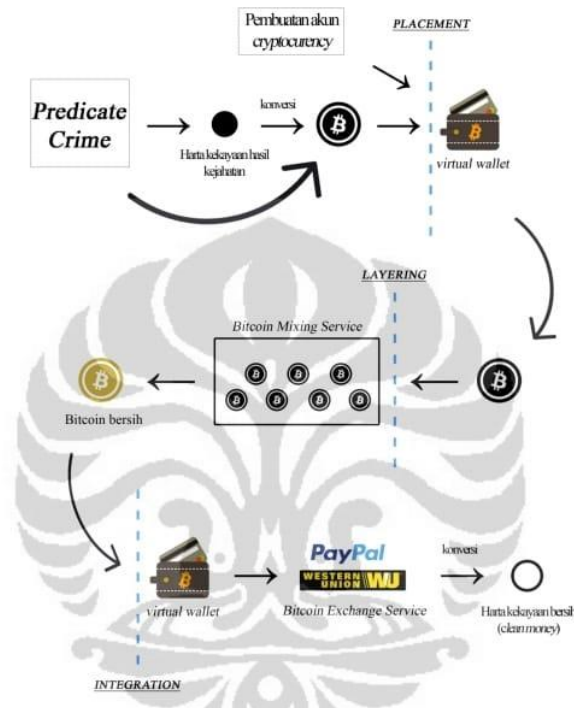


Figure 1. Stages of Cryptocurrency-Based TPPU with Examples of Bitcoin Types

1. Placement

Perpetrators of criminal acts (e.g. corruptors, bribe recipients, drug dealers, and so on) use the wealth from their criminal acts (core crime) to buy cryptocurrency, namely Bitcoin, and place it in an account (or called a Wallet) at a cryptocurrency address.

2. Layering

The perpetrators move, distribute, disguise and hide the wealth of the original criminal act through a service that provides Bitcoin Mixers (mixing Bitcoin) with a certain discount so that the traces of the origin are faint.

3. Integration

The perpetrator converts Bitcoin into legal currency using the Bitcoin Exchange method through PayPal or Western Union platforms. This exchange process certainly passes the identity verification of the required source of funds because the currency (crypto) that is exchanged has entered the legitimate financial system.

The following is a simple illustration of the stages of cryptocurrency-based TPPU:

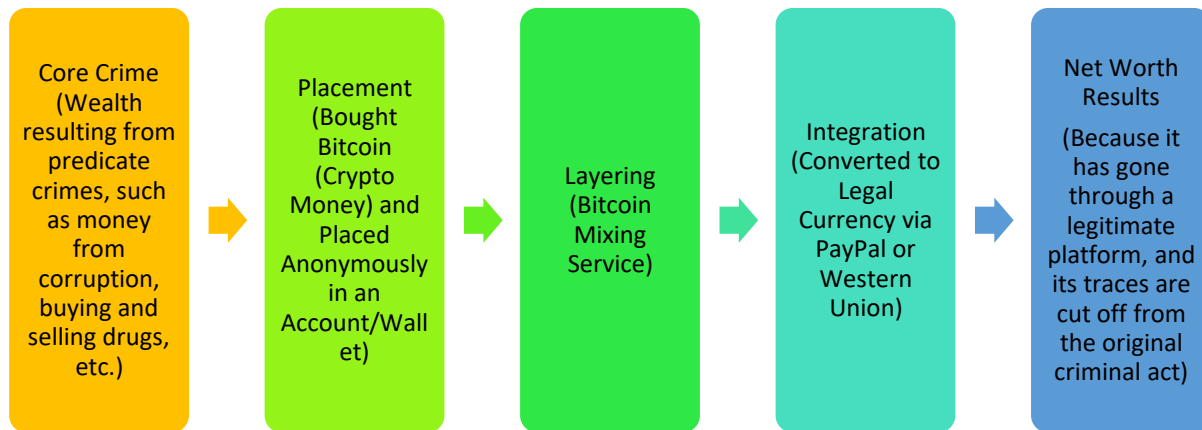


Figure 2. Stages of Cryptocurrency-Based TPPU

The absence of a trace link between the wealth of the crime's origin and the perpetrator's exchanged currency shows that cryptocurrency-based TPPU is a perfect TPPU.

Cryptocurrency-based TPPU (or another term called cyber laundering) also meets the characteristics of cybercrime. Sugiyono & Runturambi (2024), as found in the background paper for the workshop of the UN Congress X/2000 in Vienna, Austria, the term cybercrime is divided into two categories, namely: (a) cybercrime in a narrow sense is called computer crime which contains the meaning of all acts through electronic operations that target the security of computer systems and the data processed in them, and (b) cybercrime in a broad sense is called computer-related crime, Any illegal act committed by means of computer systems or networks which includes crimes such as the expropriation of property, offering or distributing information through computer system networks. The characteristics of cybercrime owned by cryptocurrency-based TPPU include the following:

1. The modus operandi is information technology, and not everyone has qualified insights related to the cyber world.
2. The perpetrator can be without identity and has no boundaries.
3. The scope is global because it can be carried out transnationally across national borders (there are no restrictions on time and place), so it is difficult to ascertain the jurisdiction of state law that applies to the perpetrator.
4. It is non-violent in the sense that the chaos caused by this crime in cyberspace cannot be seen directly like conventional criminal acts.
5. The losses incurred include material (money) and immaterial losses (data confidentiality).

Trends and Prevention of Cryptocurrency-Based Anti-Money Laundering

As mentioned at the beginning of this article, there have been cryptocurrency-based TPPU cases in Indonesia, which are not only follow-up crimes from corruption cases but also scamming, ransomware, etc. Kerr et al. (2023) data from the crypto crime report found that there were

indications of money laundering through crypto assets; this amounted to USD.8.6 billion in 2022. This is equivalent to Rp.139 trillion globally. In addition to crypto assets, several instruments that are at risk of being used by TPPU actors include virtual assets, NFTs, market activities, electronic money, and artificial intelligence (AI) used to automate transactions. It is possible that this phenomenon will continue to increase in the future.

This has not escaped the government's monitoring. President Joko Widodo urged his staff to build international cooperation, strengthen regulation and transparency, enforce the law indiscriminately and use important technology.

From the regulatory side

It has previously been explained that cryptocurrencies themselves, on the one hand, are not recognized as legal tenders, so they do not have a legal umbrella, and the risks of their use are borne by the user himself. On the other hand, cryptocurrencies are included in the list of commodities that can be used as the subject of Futures Contracts traded on the Futures Exchange because their use is expected to contribute positively to Indonesia's futures trading.

The two contradictory things about cryptocurrency regulation are then faced with a phenomenon called cryptocurrency-based TPPU. Cryptocurrency is a commodity in the realm of the capital market, where wealth from criminal acts in the capital market is one of the core crimes of TPPU. Cryptocurrencies can also be seen as a mode of TPPU. However, there are no specific rules governing this cryptocurrency-based TPPU. Based on the search related to the provisions that regulate cryptocurrency-based anti-money laundering, Article 2 of Bappepti Regulation Number 6 of 2019 concerning the Implementation of Anti-Money Laundering and Prevention of Terrorism Financing Programs Related to the Implementation of Commodity Physical Markets on the Futures Stock Exchange, which regulates the implementation of Bappepti regulations related to the implementation of anti-money laundering programs apply *mutatis mutandis* to the implementation of the Futures Exchange, Physical Commodity Traders and Physical Trading Intermediaries.

Divina (2021) is different from other countries, such as the United States, which places virtual currencies such as cryptocurrencies as Money Service Business / MSB because their value replaces currency and also as a security, not just as a commodity. So, its activities are subject to anti-money laundering/AML provisions depending on what sector is involved in these activities (Azzahra et al., 2024). As an MSB, virtual currencies are subject to the provisions of the U.S. Bank Secretary Act/BSA, with the Financial Crimes Enforcement Network (FinCEN) as its enforcer. As a security, it is subject to the provisions of the Securities and Exchange Commission/SEC. As a commodity, it is subject to the provisions of the Commodity Futures Trading Commission/CFTC. Thus narrowing the gap for criminal acts related to virtual currency. In the context of TPPU, the legal basis used in the United States is 18 U.S. Code § 1956 and the Patriot Act of 2001, which complement the BSA to identify users whether they meet the Know Your Customer/KYC

procedures (which include the Customer Identification Program/CPI and Customer Due Diligence/CDD) requirements).

In terms of law enforcement

It is undisputable that cryptocurrency-based TPPU is a criminal act that is difficult to trace by law enforcement officials, so the perpetrators can freely use the wealth for legitimate and illegal activities. Therefore, the impact of cryptocurrency-based TPPU not only threatens the stability and integrity of the economic and financial systems but can also endanger the joints of society, nation, and state life.

Meanwhile, in Indonesia, because there is no comprehensive regulation regarding cryptocurrency-based anti-corruption, there is no cooperation between law enforcement, for example, regarding anonymity investigations.

Considering this, cooperation should be carried out between Bappepti, Bank Indonesia, and the Financial Services Authority (OJK) to reveal information disclosure between law enforcement so that it can prevent the occurrence of cryptocurrency-based anti-money laundering, as is the case with MSB in the United States carried out by FinCEN in collaboration with law enforcement.

CONCLUSION

Cryptocurrency-based money laundering (TPPU) represents an ideal method of money laundering due to the lack of traceable links between the original criminal act, the perpetrator, and the exchanged currency. In Indonesia, there are no specific regulations addressing cryptocurrency-based anti-corruption, and no collaborative efforts exist among law enforcement agencies to prevent it. To address this, it is suggested that legal instruments be developed to regulate cryptocurrency-based anti-money laundering, adhering to a risk-based approach as recommended by the Financial Action Task Force (FATF). Additionally, cooperation between Bappepti, Bank Indonesia, and the Financial Services Authority (OJK) is essential to ensure information disclosure among law enforcement agencies, thereby preventing cryptocurrency-based anti-corruption.

REFERENCES

- Azarenkova, G., Shkodina, I., Samorodov, B., & Babenko, M. (2018). The influence of financial technologies on the global financial system stability. *Investment Management & Financial Innovations*, 15(4), 229.
- Azzahra, A., Savandha, S. D., & Olubisi, M. G. (2024). Effective Strategies for Corporate Governance and Risk Management in the Public Sector: Preventing Corruption and Abuse of Authority. *Asian Journal of Engineering, Social and Health*, 3(4), 911–919. <https://doi.org/10.46799/ajesh.v3i4.366>

- Borghini, M., & Katos, V. (2021). *Vendor Accounts on Third Party Trading Platforms*.
- Divina, B. P. (2021). *Tindak pidana pencucian uang melalui Cryptocurrency*.
- Fadeyi, O., Krejcar, O., Maresova, P., Kuca, K., Brida, P., & Selamat, A. (2019). Opinions on Sustainability of Smart Cities in the Context of Energy Challenges Posed by Cryptocurrency Mining. *Sustainability*, 12(1), 169. <https://doi.org/10.3390/su12010169>
- Flick, U. (2018). *Triangulation in data collection*. The SAGE handbook of qualitative data collection.
- Giungato, P., Rana, R., Tarabella, A., & Tricase, C. (2017). Current Trends in Sustainability of Bitcoins and Related Blockchain Technology. *Sustainability*, 9(12), 2214. <https://doi.org/10.3390/su9122214>
- Jacobs, G. (2018). Cryptocurrencies & the challenge of global governance. *Cadmus*, 3(4), 109–123.
- Kerr, D. S., Loveland, K. A., Smith, K. T., & Smith, L. M. (2023). Cryptocurrency Risks, Fraud Cases, and Financial Performance. *Risks*, 11(3), 51. <https://doi.org/10.3390/risks11030051>
- Kethineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*, 30(3), 325–344. <https://doi.org/10.1177/1057567719827051>
- Kim, H., Sefcik, J. S., & Bradway, C. (2017). Characteristics of Qualitative Descriptive Studies: A Systematic Review. *Research in Nursing & Health*, 40(1), 23–42. <https://doi.org/10.1002/nur.21768>
- Leech, N. L., & Onwuegbuzie, A. J. (2007). An array of qualitative data analysis tools: A call for data analysis triangulation. *School Psychology Quarterly*, 22(4), 557–584. <https://doi.org/10.1037/1045-3830.22.4.557>
- Murti, T. W., Kefianto, K., Ferdiansyah, R., Priyambodo, M. B., Akbar, M., & Nugroho, A. A. (2024). Analisa Kebijakan Hukum Terhadap Kasus Koin Kripto Sebagai Bukti Elektronik Tindak Kejahatan Pencucian Uang. *Media Hukum Indonesia (MHI)*, 2(2).
- Namey, E., Guest, G., Thairu, L., & Johnson, L. (2008). Data reduction techniques for large qualitative data sets. *Handbook for Team-Based Qualitative Research*, 2(1), 137–161.
- Rejeb, A., Rejeb, K., & Keogh, J. G. (2021). Cryptocurrencies in modern finance: a literature review. *Etikonomi*, 20(1), 93–118.
- Sugiyono, A. F., & Runturambi, A. J. S. (2024). MEMERANGI CYBERCRIME DAN TPPO PEKERJA MIGRAN INDONESIA (PMI) NON-PROSEDURAL KE KAMBOJA. *Jurnal Ilmiah Kajian Keimigrasian*, 7(1), 43–61.
- Taguchi, N. (2018). Description and explanation of pragmatic development: Quantitative, qualitative, and mixed methods research. *System*, 75, 23–32. <https://doi.org/10.1016/j.system.2018.03.010>

Analysis of the Financial Feasibility Study of Investment in Electricity Infrastructure Development Using the Monte Carlo Method Case Study of the Construction of GITET 500 kV Cikande

Vaz, J., & Brown, K. (2020). Sustainable development and cryptocurrencies as private money. *Journal of Industrial and Business Economics*, 47(1), 163–184. <https://doi.org/10.1007/s40812-019-00139-5>

Copyright holder:

Mohammad Nur Bobby Putra Yusra, Arthur Josias Simon Runturambi, Bondan Widiawan (2024)

First publication right:

Asian Journal of Engineering, Social and Health (AJESH)

This article is licensed under:

