



## Money Laundering through Cryptocurrency and Its Arrangements in Money Laundering Act

Andhira Alya Wardani<sup>1</sup>, Mahrus Ali<sup>1,\*</sup>, and Jaco Barkhuizen<sup>2</sup>

<sup>1</sup> Faculty of Law, Universitas Islam Indonesia, Yogyakarta, Indonesia

<sup>2</sup> University of Limpopo, Mankweng, Limpopo, South Africa

\*Corresponding author: [mahrus\\_ali@uii.ac.id](mailto:mahrus_ali@uii.ac.id)

**Abstract.** The development of the modus operandi of money laundering become a major concern. Cryptocurrency technology has the potential to become a new media for money laundering because law enforcement officials still use to this technology, this technology which has a pseudonymous and even anonymous character is a new means for money laundering perpetrators to disguise their crimes. This study aims to examine how cryptocurrency is used as the modus operandi of money laundering and how is the readiness of regulations in Indonesia, especially Law No. 8 of 2010 in prosecuting money laundering offenders with the cryptocurrency modus operandi. This study uses a normative juridical method with legal materials from literature studies and uses a statutory regulation approach. The results of this study are the use of crypto as a mode of money laundering due to peer-to-peer networks, namely the absence of third parties to supervise crypto transactions, high user privacy, and transaction flexibility.

**Keywords:** Modus Operandi, Cryptocurrency, Money Laundering, Indonesia

**Abstrak.** Berkembangnya modus operandi pencucian uang menjadi perhatian utama. Teknologi cryptocurrency berpotensi menjadi media baru TPPU dikarenakan masih awamnya teknologi tersebut oleh aparat penegak hukum, teknologi yang memiliki karakter pseudonymous bahkan anonymous ini menjadi sarana baru bagi pelaku TPPU untuk menyamarkan kejahatannya. Penelitian ini bertujuan untuk mengkaji bagaimana pemanfaatan cryptocurrency sebagai modus operandi TPPU dan bagaimana kesiapan regulasi di Indonesia khususnya Undang-Undang Nomor 8 Tahun 2010 dalam menjerat pelaku TPPU dengan modus operandi cryptocurrency. Penelitian ini menggunakan metode yuridis normatif dengan bahan hukum studi kepustakaan dan menggunakan pendekatan peraturan perundang-undangan. Hasil penelitian ini adalah pemanfaatan kripto sebagai modus pencucian uang dikarenakan jaringan peer-to-peer yaitu tidak adanya pihak ketiga yang melakukan pengawasan transaksi kripto, privasi pengguna yang tinggi, dan fleksibilitas transaksi.

**Kata kunci:** Modus Operandi, Cryptocurrency, Pencucian Uang, Indonesia



## 1. Introduction

Economic activity is something that cannot be separated from human interaction. To turn the wheels of the economy, money becomes an important part in it. In economics, money is defined as a generally accepted medium of exchange.<sup>1</sup> Along with the rapid progress and development of existing technology and the birth of many innovations to facilitate human activities, especially in the financial sector which allows transactions to be carried out easily and can be done anywhere.<sup>2</sup>

The development of technology triggers the emergence of many innovations, one of which is in the field of banking, namely the use of currency in digital form. This method replaces manual transactions using cash, replaced by using virtual money. One form of virtual currency that is quite popular in Indonesia is a form of cryptocurrency, namely Bitcoin. Cryptocurrency or Cryptocurrency is a digital currency that is created and managed using sophisticated encryption techniques known as cryptography. This currency was discovered by Satoshi Nakamoto in 2009, he released a software better known as Bitcoin on the internet<sup>3</sup>.

On the other hand, technological developments have had a positive impact, this innovation has also opened up opportunities for criminals to use it as a tool to commit crimes, one of which is money laundering. This new mode of money laundering takes advantage of the development of innovation in the field of cyber which can also be called cyber laundering, where the implementation uses internet-based electronic transfers in order to disguise illegal sources of funds<sup>4</sup>.

Perpetrators can carry out their actions easily anytime and anywhere, the use of this mode is due to two reasons, namely first that virtual money payments can be made anonymously or pseudonymously which results in the circulation of money not being tracked easily and can move quickly, making it difficult to apply conditions reporting and tracking (audit trail) to track. Then, the second reason is that virtual money transfers make it possible to be carried out without the intervention of third parties (financial institutions) or peer to peer, so the speed and anonymity of electronic transfers makes it difficult for law enforcement to track traces of money obtained illegally<sup>5</sup>.

---

<sup>1</sup> Supramono, Gatot. *Hukum Uang di Indonesia*. Bekasi: Gramata Publishing, 2014.,

<sup>2</sup> Alfitra, A. (2014). *Modus Operandi Pidana Khusus di Luar KUHP: korupsi, money laundering, & trafficking*. Jakarta: Raih Asa Sukses, 2014.

<sup>3</sup> Nurbaiti, Siti. "Kedudukan Hukum Bitcoin Sebagai Mata Uang Virtual Di Indonesia Berdasarkan Undang-Undang Nomor 7 Tahun 2011 Tentang Mata Uang." *Jurnal Hukum Adigama* 1, no. 1 (2018): 1403-1428.

<sup>4</sup> Amrani, Hanafi. *Hukum Pidana Pencucian Uang*. Yogyakarta: UII Press, 2015.

<sup>5</sup> McJohn, Stephen M., and Ian McJohn. "The Commercial Law of Bitcoin and Blockchain Transactions." *Uniform Commercial Code Law Journal, Forthcoming, Suffolk University Law School Research*

Cryptocurrency in Indonesia does not yet have legal certainty in its use as a transaction tool, but in the Regulation of the Minister of Trade (Permendag) No. 99 of 2018 concerning the General Policy for Organizing Crypto Asset Futures Trading, cryptocurrency is defined as a commodity traded on futures exchanges.<sup>6</sup> The circulation of cryptocurrency is issued by private parties so that there is no formal institution that supervises the course of transactions, so that the freer use of cryptocurrency is very vulnerable to being used as a medium for money laundering.

Law No. 8 of 2010 concerning the Prevention and Eradication of Laundering Crimes has not explicitly regulated the use of cryptocurrency, in particular burdening currency exchange service providers (bitcoin exchange money) as reporting parties, who have the obligation to carry out reporting, monitoring compliance and application of the principle of knowing your customer and making it easier for law enforcement officials to eradicate money laundering crimes<sup>7</sup>. Thus, it becomes an interesting issue to analyze and examine the modus operandi of money laundering through virtual currency (cryptocurrency) and its regulation in Indonesian money laundering laws.

## 2. Research methods

The research method that researchers use is to use normative juridical, by using literature studies and laws and regulations. In conducting data analysis, this study used a qualitative research approach to gain understanding and explain complex problems. In analyzing and reviewing data, this research is assisted by primary legal materials, laws and regulations, secondary legal materials, which consist of books, journals or research results related to research and analysis of legal theory related to the problem of the research researcher, as well as opinions from legal experts, as well as tertiary legal materials such as electronic data, KBBI, legal language dictionaries.

---

*Paper* 16-13 (2016). See also, Prayogo, Galang, and Yuliia Chornous. "Conceptualization of Future Cryptocurrency Laws in Indonesia and Ukraine." *Lex Publica* 7, no. 2 (2020): 56-68.

<sup>6</sup> Regulation of the Minister of Trade (Permendag) No. 99 of 2018 concerning General Policy for Organizing Crypto Asset Futures Trading.

<sup>7</sup> Parwoto, Adi, Evi Deliana, and Ferawati Ferawati. "Analisis Yuridis Penggunaan Mata Uang Virtual (Bitcoin) Sebagai Sarana Tindak Pidana Pencucian Uang (Money Laundering)." *Jurnal Online Mahasiswa (JOM) Bidang Ilmu Hukum* 6, no. 2 (2019): 1-15.

### 3. Research Results and Discussion

#### 3.1. Modus Operandi of Money Laundering Crimes Utilizing Cryptocurrency

In the past, the existing money laundering model used conventional methods with fiat currency, namely currency issued by the government and regulated through the laws of a country.<sup>8</sup> Money from crime will be entered into a financial system and will mix with the circulation of legal money so that it can disguise the illegal money. Money laundering is becoming an increasingly complex problem at this time. This is because it is increasingly difficult to prove the mode and system of crime used by the perpetrators, because it involves technological sophistication whose movements and developments are difficult for law enforcement officials to follow.

Several money laundering cases have used Cryptocurrency as a medium for perpetrators to deceive the authorities for the proceeds of their crimes. this utilization is carried out by actors due to the unique system that is owned by Virtual Currency (Cryptocurrency). Following is the data that researchers have summarized in several cases that used Virtual Currency or Cryptocurrency as the modus operandi of money laundering.

##### 4.1.1. Brazilian Illegal Gold Mining Criminal Group

A criminal group in Brazil has been mining gold since 2012 where this activity does not use a valid environmental permit. This criminal group uses tokens created by a shell company to move crypto tokens worth millions of dollars, banking analysts from the Brazilian federal police stated that from 2019 to 2021, 16 million reais or \$ 3 billion were transferred through the group's bank accounts<sup>9</sup>. The modus operandi used is as follows.

1. Placement Receiving proceeds from illegal gold mining and placing them in a group bank account.
2. Layering Create a company and crypto tokens on behalf of the company, then manage the money from the results of these illegal activities to be converted into Crypto so that it looks like the results of legitimate activities
3. Integration The proceeds of crime that are in the company's crypto tokens are as if they were invested and the dividends obtained came from third party investments

---

<sup>8</sup> Wijaya, Dima Ankaa, and Oscar Darmawan. *Blockchain Dari Bitcoin Untuk Dunia*. Jakarta: Jasakom, 2017.

<sup>9</sup> Reuters. *Brazil police raids gang allegedly using crypto to launder illegal gold mining*. July 8, 2022. Retrieved from <https://www.reuters.com/world/americas/brazil-police-raids-gang-allegedly-using-crypto-launder-illegal-gold-mining-2022-07-07/>.

#### **4.1.2. Liberty Reserve case**

In 2013 a money transmitting service provider was established where the company was called Liberty Reserve. This service provider company claims that the payment system owned by their company is the oldest, safest, and very popular. In conducting money exchange transactions, users only need name, address and date of birth and are not required to verify user identity. Users usually exchange their cash into digital money with the facilities provided by Liberty Reserve and with this instant process digital money will be converted back into cash. That this transfer scheme has processed 78 million transactions with a value of up to \$ 8 billion, of which the amount is the concealment of the results of Ponzi fraud, hacking, credit card theft and identity fraud. Liberty Reserve provides money transfer services to facilitate money laundering on a massive scale, this is because they utilize an anonymous transaction process, difficult to track and easy to transfer<sup>10</sup>. The modus operandi used is as follows:

1. Placement Receiving the proceeds of a crime to be placed in a digital currency (Cryptocurrency) system.
2. Layering Convert digital currency back into cash or send it to another account, where previously the digital currency was cash from a crime proceeds

#### **3.1.3. ASABRI Corruption and Money Laundering Case**

Asabri's investment and finance director and investment division head Adam Rachmat Damiri made an agreement with Asabri's outsiders, namely one of them Heru Hidayat as PT Trada Alam Minera to buy and exchange shares in Asabri's portfolio with shares owned by Heru Hidayat at a manipulated price to be high with the aim of performance Asabri's portfolio appears to have high value and is liquid. Re-placement of investment funds in stocks or other investments that do not meet the requirements, and based on Heru Hidayat's recommendation to place PT ASABRI funds in mutual funds to be managed by several investment managers, which eventually become risky and illiquid shares so that they do not provide benefits to PT ASABRI<sup>11</sup>. The modus operandi used is as follows.

1. Placement, buying a number of bitcoins from PT Indodax Nasional Indonesia from money resulting from corruption at PT ASABRI.
2. Layering, Bitcoin purchase transaction Using a nominee (other person's name) to create a bitcoin account/token

---

<sup>10</sup> Kainama, Maria Minerva, Nuswantoro Dwi Warno, and Joko Setiyono. "Pencegahan Dan Penindakan Penggunaan Virtual Currency Sebagai Sarana Kejahatan Pencucian Uang Melalui Dunia Maya (Studi Kasus Liberty Reserve)." *Diponegoro Law Journal* 6, no. 1 (2017): 1-13.

<sup>11</sup> Merdeka. *Kronologi Terkuaknya Kasus Korupsi Asabri Terbesar Sepanjang Sejarah Indonesia*. Feb 7, 2021. Retrieved from <https://www.merdeka.com/uang/kronologi-terkuaknya-kasus-korupsi-asabri-terbesar-sepanjang-sejarah-indonesia.html>.

Cryptocurrency has a system that utilizes cryptographic technology as a security system and blockchain technology as a data storage system. Most Cryptocurrencies use the same technology, and require things like a pair of keys (public and private), wallets (wallets), miners (miners), and a decentralized network (peer-to-peer).<sup>12</sup>

Cryptographic technology in bitcoin uses public keys and private keys mechanisms to carry out online transactions<sup>13</sup>. Every transaction will be protected by an online signature, these public keys function as “addresses”, which users use to send Cryptocurrency units. Meanwhile, private keys are kept secret and function to claim the ownership of a Cryptocurrency unit from the user<sup>14</sup>. Even though the bitcoin address is communicated to everyone, only the owner of the address who has the private key can claim the crypto in that address.<sup>15</sup> By using cryptographic techniques, if the owner of the bitcoin address will use the money, the bitcoin system will determine whether the owner has a private key that matches the bitcoin address (public keys).<sup>16</sup>

Discussing cryptocurrency cannot be separated from blockchain technology. Blockchain is a technology used in the field of insurance and financial service providers. commonly used in trade financing, payroll and insurance payments, banks, brokerages, exchanges, investments, merchants, compliance trading platforms, capital markets, money services, and others<sup>17</sup>.

Distributed Ledger Technology (DLT) is the main foundation of a blockchain technology, this technology offers a validation consensus through a computer network with peer-to-peer transactions, namely a transaction without the need for intermediaries or a central authority to update and maintain information originating from transactions<sup>18</sup>. blockchain is basically a distributed database record, public ledger (public ledger) of all transactions, every transaction that has been distributed to each participant, in the public ledger will be verified by consensus by the majority of participants in the system<sup>19</sup>.

Distributed Consensus (Consensus validation) in blockchain technology allows every online transaction that includes digital assets to be verified at any time, this

---

<sup>12</sup> Conway, Joey. *Beginners Guide to Cryptocurrencies*. Personal blog, May 19, 2014. Retrieved from <https://www.joeyconway.com/blog/wp-content/uploads/2014/10/Beginners-Guide-to-Cryptocurrencies-final.pdf>.

<sup>13</sup> Crosby, Michael, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. “Blockchain technology: Beyond bitcoin.” *Applied Innovation* 2, no. 6-10 (2016): 71.

<sup>14</sup> Conway, *Beginners Guide to Cryptocurrencies*, p. 3.

<sup>15</sup> Wijaya, Dimaz Ankaa. *Mengenal Bitcoin & Cryptocurrency*. Medan: Puspantara, 2016.

<sup>16</sup> *Ibid.*

<sup>17</sup> Lee, David Kuo Chuen, and Linda Low. *Inclusive FinTech: Blockchain, Cryptocurrency and ICO*. Singapore: World Scientific Publishing Co. Pte. Ltd., 2018.

<sup>18</sup> Rennock, Michael JW, Alan Cohn, and Jared R. Butcher. “Blockchain technology and regulatory investigations.” *Practical Law Litigation* 1 (2018): 35-44.

<sup>19</sup> Crosby et al., “Blockchain technology...”, p. 8.



without offending the privacy of the parties involved, so that Distributed Consensus and Anonymity are two important characteristics in blockchain technology<sup>20</sup>. This decentralized system prevents interference from authorities such as the central bank or government. The public ledger or blockchain in the Cryptocurrency system provides transparency in transactions, which is important when building trust between parties who previously did not trust each other.<sup>21</sup>

Bitcoin has high flexibility, because the transaction does not require identity verification or certain requirements<sup>22</sup>. Bitcoin is designed with a privacy model in which transactions made and addresses owned by a user have no direct connection with the real identity of the owner, this is because there is no centralized controlling organization in the bitcoin system that controls users and transactions that occur within the system.<sup>23</sup>

Although the blockchain system within bitcoin allows ongoing transactions to be seen by everyone, the identities associated with transactions remain hidden<sup>24</sup>. This explains that bitcoin account ownership is complex and anonymous, because the public keys owned by each user cannot be tracked easily because there are periodic changes, so that the user in each transaction will not be the same.<sup>25</sup>

Bitcoin has a distributed system, peer-to-peer network. The bitcoin system does not have a central network controller, and has a system where all nodes in the network have the same position. Each transaction to transfer a certain number of bitcoins between users is transmitted to the bitcoin network where it is stored in the blockchain distributed transaction ledger.<sup>26</sup> Before a transaction is forwarded, each node first verifies the transaction, which includes checking the syntax and structure, and whether it is a valid transfer of the unspent amount of the transaction output<sup>27</sup>.

Valid transactions will be added to the blockchain in a process known as bitcoin mining, each node will collect valid transaction numbers into a block and will try to calculate the cryptographic hash of the block, the first node to find the hash wins the block, which means the block will be entered into blockchain and deployed to the network<sup>28</sup>. When a node receives a new valid block, it will stop the

---

<sup>20</sup> *Ibid.*

<sup>21</sup> Conway, *Beginners Guide to Cryptocurrencies*,

<sup>22</sup> *Ibid.*

<sup>23</sup> Wijaya, Dimaz Ankaa. *Bitcoin Tingkat Lanjut*. Medan: Pusantara, 2016, p. 50.

<sup>24</sup> *Ibid.*

<sup>25</sup> Saragih, Abraham. "Bitcoin dalam Perspektif Kejahatan Siber: Analisis Kriminologi berbasis posmodern." *Jurnal Kriminologi Indonesia* 15, no. 1 (2020).

<sup>26</sup> Vranken, Harald. "Sustainability of bitcoin and blockchains." *Current opinion in environmental sustainability* 28 (2017): 1-9.

<sup>27</sup> *Ibid.*

<sup>28</sup> *Ibid.*

mining process for the current block and start mining a new block, the node that won the block will get a block reward in the form of bitcoins.<sup>29</sup>

In the bitcoin system, which will be stored in an internet network, but no one can spend these bitcoins without the owner's knowledge<sup>30</sup>. This is due to the function of the key of the cryptographic system (public and private key), the private key acts like an ATM PIN combination, where maintaining its secrecy is very important because only that can be proof of ownership of bitcoins owned<sup>31</sup>.

Calculations to look up and verify the cryptographic hash of a block When bitcoin mining, allows the bitcoin network to gain consensus on the status of transactions. This process of bitcoin mining decentralizes the issuance of currency and clearing transactions which are usually carried out by central banks and clearing houses<sup>32</sup>.

The various features offered by the technology behind the Cryptocurrency are related to the theory that someone who commits a crime experiences pressure in the physical space, will have a tendency to commit crimes in cyberspace, this is because physical space limits movement to commit crimes.<sup>33</sup>. To explain the use of bitcoin as a *modus operandi* for laundering, this can be explained with a multidimensional approach by combining various fields such as criminology, victimology, sociology, internet network science, and computer science. As Jaishankar (2008) quoted from Abraham Saragih describes seven postulates in the Space Transition Theory, where the seven postulates are related to the behavior of using bitcoin as a mode of crime. Here are the seven postulates:<sup>34</sup>

1. Someone who has pressure in the physical space when committing a crime will tend to take advantage of the cyber sphere because of the status they have. This can be seen how criminals use cryptocurrency as a money laundering tool, from the results of their illegal activities. And because it is decentralized so that supervision escapes the authorities.
2. Due to the flexibility of identity, dissociative anonymity and the lack of prevention against cyber crime, it opens up space for perpetrators to take advantage of this gap to commit crimes. The anonymity possessed by bitcoin or other cryptocurrencies makes it easier for perpetrators to carry out illegal activities. And the use of sophisticated technology by criminals, such as hiding IP addresses, to trick or escape from the authorities, makes it increasingly difficult to track cybercriminals.

---

<sup>29</sup> *Ibid.*

<sup>30</sup> Wijaya, *Mengenal Bitcoin & Cryptocurrency*, p. 16.

<sup>31</sup> *Ibid.*

<sup>32</sup> *Ibid.*

<sup>33</sup> Saragih, "Bitcoin dalam Perspektif Kejahatan Siber..."

<sup>34</sup> *Ibid.*, p. 6.



3. Behavior within the cyber space can be carried over to the physical space and vice versa. It can be exemplified how the proceeds of crime in the form of various currencies can be brought into cyberspace, namely bitcoin, and there is a continuous circulation between legal currency and bitcoin.
4. The actions that are irregular (do not have a definite time) from the perpetrator are spatio-temporal dynamic in that they provide an opportunity to escape. Cybercriminals, of course, take advantage of cybersecurity loopholes in an effort to prevent them from being tracked down quickly.
5. Cybercriminals will usually not show their real identities, and this also applies when they interact with each other. So that anonymity is very much needed and important for them to avoid the various risks they might experience.
6. People from countries that limit their people to do many things have a greater possibility of committing cyber crimes.
7. Conflicts between values and norms that exist in the real world and the scope of cyber can lead to cyber crimes. Cyberspace users who cannot carry out illegal activities in physical space have a tendency to use cyberspace as the modus operandi of their illegal activities. This is due to the difference in consensus between cyberspace and the real world in carrying out illegal activities.

Based on the seven prostitutes above, it can be seen that bitcoin as a new medium for money laundering is due to the absence of an authority that regulates the rate of transactions and its anonymous or unknown ownership. So that this is the main factor for criminals to take advantage of these loopholes to launder their illegal money in cyberspace by using bitcoin or other cryptocurrencies, then converting them into other forms of assets without the knowledge of law enforcement officials.

### **3.2. How The Act Reaches Out to Money Laundering Using Cryptocurrency**

The circulation of cryptocurrency in Indonesia is fairly new, the legal validity of cryptocurrency itself raises many questions because its use is currently quite high. The following are the regulations that address cryptocurrency distribution in Indonesia. First, Bank Indonesia Regulation (PBI) No. 18/40/PBI/2016 Concerning Implementation of Payment Transaction Processing

Parties wishing to establish a payment company for a non-bank institution as a provider of financial system services are required to obtain a permit as stated in Article 4 Paragraph (1). Based on Article 34 Payment System Service Providers are prohibited:<sup>35</sup>

---

<sup>35</sup> Bank Indonesia Regulation No. 18/40/2016 concerning Implementation of Payment Transaction Processing.

1. Processing payment transactions using Virtual Currency
2. Misusing customer data and information as well as payment transaction data and information; and/or;
3. Possessing and/or managing a value that can be equated to the value of money that can be used outside the scope of the payment system service provider.

Second, Bank Indonesia Regulation No. 19/12/PBI/2017 concerning Implementation of Financial Technology. This regulation formulates the existence of a regulatory sandbox, namely a test room to test the implementation of financial technology together with products, services, technology, and business models that are suitable for use by the public. Article 8 Paragraph (2) Bank Indonesia Regulation No. 19/12/PBI/2017 concerning the Implementation of Financial Technology explains that apart from the obligations referred to in Paragraph (1), financial technology operators are prohibited from using payment system activities using virtual currency<sup>36</sup>.

CoFTRA Regulation No. 3 of 2020 concerning the Third Amendment to CoFTRA Regulation No. 5 of 2019 concerning Technical Provisions for Organizing the Physical Crypto Asset Market on the Futures Exchange

Article 5 Paragraph 1 CoFTRA Regulation No. 3 of 2020 states that circulation of crypto assets must be traded through futures exchanges that have met the approval of CoFTRA. As in Article 24 Paragraph (8) letter b which reads:<sup>37</sup>

“Prospective crypto asset physical traders who carry out their activities during the registration period must pay attention to the following provisions: (b) must implement anti-money laundering and prevention of terrorism financing and proliferation of weapons of mass destruction programs stipulated by CoFTRA.”

The regulation reminds prospective traders of physical crypto assets as traders of crypto assets on futures exchanges to implement an anti-money laundering program<sup>38</sup>. The regulation above confirms that the existence of cryptocurrency in Indonesia is not recognized as a means of payment, but as a commodity asset. However, there are no further regulations regarding the anti-laundering program in trading crypto assets on futures exchanges.

The use of cryptocurrency as a medium for money laundering, to realize the perpetrator's goal of disguising the funds and information on the source of the

---

<sup>36</sup> Bank Indonesia Regulation No. 19/12/PBI/2017 concerning Implementation of Financial Technology.

<sup>37</sup> CoFTRA Regulation No. 3 of 2020 concerning Technical Provisions for Organizing Physical Trading of Crypto Assets on Futures Exchanges.

<sup>38</sup> Trisakti, Anton Jaksa, and Eko Soponyono. “Upaya Pencegahan Tindak Pidana Pencucian Uang Dalam Bentuk Uang Kripto (Bitcoin) Menggunakan Prinsip Kehati-Hatian Perbankan.” *Jurnal Belo* 7, no. 1 (2021): 37-54.

money<sup>39</sup>. Apart from that, there is still a lack of regulations governing its circulation, creating a loophole for criminals to carry out their crimes, this is because there is no institution that can oversee the existence of this cryptocurrency.

The formulation of elements or forms of money laundering offenses consists of objective elements (*actus reus*), namely actions in the form of placement, layering and integration.<sup>40</sup> As well as the subjective element (*mens rea*) where the actions of a person who knows or should be suspected of originating from an unlawful act but deliberately hide or disguise the illegal money<sup>41</sup>. Referring to Law No. 8 of 2010 concerning Prevention and Eradication of Money Laundering Crimes, TPPU can be divided into 2, namely active money laundering and passive money laundering.

In Articles 3 and 4, the formulation of active money laundering actors, active offenses are carried out in the form of actions, both formulated materially and formally. the perpetrator performs an active action by violating the prohibition, where the active action must be marked by a body movement<sup>42</sup>. The formula is specified in Chapter 3 that "Anyone who places, transfers, diverts, spends, pays, grants, deposits, takes abroad, changes form, exchanges with currency or securities or other actions on Assets that he knows or reasonably suspects is the result of a criminal act as intended in Article 2 paragraph (1) with the aim of concealing or disguising the origin of assets, the criminal act of money laundering is punishable by imprisonment for a maximum of 20 (twenty) years and a fine of up to IDR 10,000,000,000.00 (ten billion rupiah)."

Moreover, Chapter 4 stated that "Anyone who hides or disguises the origin of the source, location, designation, transfer of rights, or actual ownership of assets which he knows or reasonably suspects are the proceeds of a crime as referred to in Article 2 Paragraph (1) shall be punished for the crime of laundering. money with a maximum imprisonment of 20 (twenty) years and a maximum fine of IDR 5,000,000,000.00 (five billion rupiahs)"

The formulation of criminal acts in Article 3 is intended to ensnare money laundering perpetrators who are also perpetrators of predicate crimes or who make money from the crimes they have committed. Then Article 4 is a form of active money laundering, but what distinguishes it from Article 3 is the form of the

---

<sup>39</sup> Sam, Y. A. B. L., Messy Rachel Mariana Hutapea, and Suyudi Setiawan. "Legalitas Cryptocurrency dalam Tindak Pidana Kejahatan Pencucian Uang." *Jurnal Ilmu Hukum* 18, no. 1 (2022): 108-120.

<sup>40</sup> Ardiano, Chandra, Pujiyono Pujiyono, and Nur Rochaeti. "Analisis Yuridis Kriminologis Penggunaan Mata Uang Elektronik Bitcoin Sebagai Sarana Tindak Pidana Pencucian Uang." *Diponegoro Law Journal* 11, no. 1 (2022), p. 11

<sup>41</sup> *Ibid.*

<sup>42</sup> Ali, Mahrus, and Deni Setya Bagus Yuherwan. *Delik-Delik Korupsi*. Jakarta: Sinar Grafika, 2020, p. 3. See also, Amrani, Hanafi, and Mahrus Ali. "A new criminal jurisdiction to combat cross-border money laundering." *Journal of Money Laundering Control* 25, no. 3 (2022): 540-550.

element of action (*feit*) and the element of intent (*oogmerk*).<sup>43</sup> Whereas in Article 4 it is aimed at actions that are not directly related to assets but the actions taken have the effect of hiding or disguising the results of criminal acts<sup>44</sup>. So that Article 4 is intended to ensnare parties that help or facilitate indirectly in fund transactions<sup>45</sup>. Moreover, in Article 5 it defines passive money laundering perpetrators and emphasizes the imposition of criminal sanctions on a person or financial service provider who enjoys assets resulting from crime or accommodates money laundering carried out by a money laundering actor and knows about suspicious transactions and does not report them as in Article 5 paragraph (2) with the reporting party listed in Article 17 paragraph (1).<sup>46</sup>

Chapter 5 stated that “Everyone who receives or controls the placement, transfer, payment, gift, donation, safekeeping, exchange, or use of assets which he knows or reasonably suspects constitute the proceeds of crime as referred to in Article 2 Paragraph (1) shall be punished with imprisonment for a maximum of 5 (five) years and a maximum fine of IDR 1,000,000,000.- (one billion rupiah)”

The explanation of the criminal elements in each article is as follows:

a. Person element

What is meant by “everyone” as a subject in the TPPU law is listed in Article 1 what is meant by “everyone” is an individual or a corporation. The crime of money laundering through Cryptocurrency is a crime that is within the scope of cybercrime, this is because various types of transaction processes run through information technology.

All activities that utilize information technology in cyberspace (cyberspace) are monitored by Law No. 19 of 2016 concerning Information and Electronic Transactions (ITE Law)<sup>47</sup>. The use of Cryptocurrency as a medium for money laundering violates the provisions of the ITE Law because both citizens and foreigners can be charged with the ITE Law, for committing acts against the law by using electronic media<sup>48</sup>.

b. Objective Elements

Law No. 8 of 2010 defines money laundering into 3 types of perpetrators, viz:

---

<sup>43</sup> Putra, Ade Riyanda Prasetya. “Problematisasi Analisis Ekonomi Terhadap Hukum Tindak Pidana Pencucian Uang.” *Lex Renaissance* 4, no. 2 (2019): 303-316.

<sup>44</sup> Kristiana, Yudi. *Pemberantasan tindak pidana pencucian uang: Perspektif hukum progresif*. Yogyakarta: Thafa Media, 2015.

<sup>45</sup> Putra, “Problematisasi Analisis Ekonomi...”

<sup>46</sup> *Ibid.*

<sup>47</sup> Wijaya, Firda Nur Amalina. “Bitcoin sebagai digital asset dalam transaksi elektronik di Indonesia (studi pada PT. Indodax Nasional Indonesia).” Master thesis, Universitas Airlangga, 2019.

<sup>48</sup> Utami, Suci. “Tindak Pidana Pencucian Uang Terhadap Uang Virtual Money Laundering on Virtual Money.” *Al-Adl: Jurnal Hukum* 13, no. 1 (2021): 1-27.

1. placing, transferring, diverting, spending, paying, granting, depositing, taking abroad, changing forms, exchanging with currency or securities with the aim of hiding or disguising origins.
2. hiding or disguising the origins of sources, locations, allocations, transfer of rights, or actual ownership of assets that he knows or reasonably suspects are proceeds of crime.
3. receive or control the placement, transfer, payment, grant, donation, safekeeping, exchange, or use of assets that he knows or reasonably suspects are proceeds of crime

Cryptocurrency is a digital asset or defined by the government as a commodity that can be traded on a futures exchange. Referring to Article 499 BW and the definition of digital assets, Cryptocurrency is included in Article 505 BW, namely movable objects which due to their nature can be moved independently or can be moved. Cryptocurrency has the characteristics of being digital and cannot be owned physically, so it is concluded that Cryptocurrency is a movable object and is an intangible object.<sup>49</sup>

c. Subjective Element

The criminal act of money laundering described in Article 3, Article 4 and Article 5 has a subjective element, especially in the words “Assets that he knows or reasonably suspects are the proceeds of a crime.”<sup>50</sup> *Mens rea* that must be proven by law enforcers, namely knowing or reasonably suspecting and intending. This element relates to the perpetrator knowing the source of the crime funds and the perpetrator wanting to make a transaction<sup>51</sup>. The difficulty that is then encountered when money laundering is carried out through Cryptocurrency is to prove the point of hiding that is done on this information technology<sup>52</sup>.

The application of the right article to the perpetrator, of course, needs to look at the elements that are carried out. With the description of the elements above, if someone is going to process the proceeds of a crime into the financial system of a Financial Service Provider to hide the results of a crime, then it is in the form of a placement, in this case changing the proceeds of a crime into any form of cryptocurrency that aims to disguise the results of a crime in the form of cryptocurrency. The next stage is to eliminate the origins of the proceeds of crime by layering, namely layering assets by sending a number of cryptocurrencies to accounts with different/fake identities or anonymous accounts. Finally, in the

---

<sup>49</sup> Wijaya, “Bitcoin sebagai digital...”, p. 128.

<sup>50</sup> Krisnamurti, Hana. “Pembuktian Tindak Pidana Pencucian Uang.” *Wacana Paramarta: Jurnal Ilmu Hukum* 14. 1 (2015).

<sup>51</sup> Utami, “Tindak Pidana Pencucian Uang...”, p. 16.

<sup>52</sup> *Ibid.*

integration stage, in this stage, the perpetrator enjoys or uses the assets resulting from the proceeds of crime as if the assets came from lawful/legal proceeds.

So that a conclusion can be drawn, if someone has committed an action that fulfills the elements of the article described above, in this case the perpetrator actively either directly or indirectly launders the proceeds of crime using cryptocurrency media, with the aim of hiding or disguising wealth. proceeds of crime can be prosecuted in Article 3 or Article 4 of Law No. 10 of 2010. Meanwhile, if an individual or corporation receives crypto currency or knows/reasonably suspects of receiving crypto currency from other people from the proceeds of crime can be charged using Article 5 of Law No. 10 Concerning Prevention and Eradication of Money Laundering Crimes.

However, the use of the TPPU Law as the main instrument for combating money laundering through Cryptocurrency is not enough. As a preventive action and to ensnare perpetrators who commit crimes within the scope of cyber, regulations are needed that help the TPPU Law to ensnare perpetrators of criminal acts, namely Law No. 19 of 2016 concerning Information and Electronic Transactions. Then the thing that needs to be done is updating in Law No. 8 of 2010, especially in Article 17 relating to the application of the know your customer (KYC) principle. This principle is a recommendation issued by the Basel committee on banking supervision and is also contained in Bank Indonesia Regulation No.14/27/PBI/2012 concerning the Anti-Money Laundering and Prevention of Terrorism Funding Program for Commercial Banks known as Enhanced Due Diligence (EDD).<sup>53</sup>

Through Bappebti regulation no. 331/BAPPEBTI.4/PENG/04/2020 there are 9 (nine) companies selling crypto assets that have been registered by CoFTRA, including, PT Crypto Indonesia Berkat, PT UPBIT Exchange Indonesia, PT Tiga Inti Utama, PT Indodax Nasional Indonesia, PT Pintu Kemana Saja, PT Zipmex Enchange Indonesia, PT Bursa Kripto Prima, PT Luno Indonesia Ltd. and, PT Rekeningku Dotcom Indonesia.<sup>54</sup>

In this regulation there are 9 (nine) financial service providers registered by CoFTRA as a form of guaranteeing legal certainty in the community that these service providers can be trusted and are under legal regulations in Indonesia.<sup>55</sup> The company has established standard account opening procedures by implementing the KYC (know your customer) principle and applying the anti-money laundering principle. However, these regulations are still limited to registered companies<sup>56</sup>.

Article 17 in Law No. 8 of 2010 explains that goods and/or service providers or other financial service providers, such as banks, are required to report to the

---

<sup>53</sup> Trisakti and Soponyono, "Upaya Pencegahan Tindak Pidana Pencucian...", p. 48.

<sup>54</sup> Ardiano et al., "Analisis Yuridis Kriminologis Penggunaan Mata Uang Elektronik Bitcoin...", 17

<sup>55</sup> *Ibid.*

<sup>56</sup> *Ibid.*



financial transaction reporting and analysis center (PPATK) regarding suspicious transactions as regulated in Article 18 Paragraph (3). The application of the principles in the Money Laundering Law is limited to 16 financial service provider institutions and 5 goods and/or service providers as stated in Article 17. Inclusion of asset traders or crypto exchanges as institutions that are required to apply the principle of customer due diligence and reporting to PPATK for suspicious transactions is a preventive measure against a new mode of money laundering, especially through cryptocurrency.

## **5. Conclusion and Suggestion**

The results showed that the development of technology, especially with the emergence of cryptocurrency as a new trend in the banking sector, is like two sides of a coin, on the other hand it brings benefits but the other side can become a new mode by money launderers to disguise or hide the proceeds of crime. The main factors for perpetrators to hide their crimes through cryptocurrency are some.

The first is A peer-to-peer network where the sending and receiving parties will be connected without a central network controller or third party as a transaction supervisor. The second is transactions that are pseudonymous or anonymous, which makes the circulation of transactions in cryptocurrency difficult to track, although they are not always anonymous and traceable, need proper handling. The third is cryptocurrency has a public key scheme and private keys, where this scheme takes into account the privacy of the user. Address identities (public keys) are not related to real identities because they can be changed every new transaction and only the owner of the private keys can access bitcoin ownership. The last is that it has flexibility, that is, does not require identity verification and can be done anywhere.

Indonesian Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes can ensnare perpetrators of money laundering through cryptocurrency if it fulfills the elements contained in the TPPU Law. Whereas perpetrators of money laundering with cryptocurrencies with the intention to disguise or hide assets resulting from criminal acts either directly or indirectly can be subject to Article 3 or Article 4 of Law No. 8 of 2010, while perpetrators who receive assets in the form of cryptocurrency or know regarding these assets originating from the proceeds of a crime, they can be charged with Article 5 of Law No. 8 of 2010.

As suggestion, renewal of Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes, is currently needed to eradicate the new mode of money laundering, especially through cryptocurrency media. The urgency of reform in Article 17 is very important with regard to the inclusion of financial

service providers such as crypto asset traders or crypto exchanges as institutions that are required to apply the Know Your Customer (KYC) principle or Customer Due Diligent, who are then obliged to report various suspicious transactions of their users so that there are steps. preventive actions carried out to eradicate money laundering crimes with the new mode. Moreover, making regulations regarding the rate of cryptocurrency transactions in Indonesia needs to be considered by the government because, with the development of the times and technology, there are more and more modes that can be used by criminals so that it is hoped that the law in Indonesia can also catch up with developments that are happening.

## References

- Alfitra, A. (2014). *Modus Operandi Pidana Khusus di Luar KUHP: korupsi, money laundering, & trafficking*. Jakarta: Raih Asa Sukses, 2014.
- Ali, Mahrus, and Deni Setya Bagus Yuherwan. *Delik-Delik Korupsi*. Jakarta: Sinar Grafika, 2020.
- Amrani, Hanafi, and Mahrus Ali. "A new criminal jurisdiction to combat cross-border money laundering." *Journal of Money Laundering Control* 25, no. 3 (2022): 540-550.
- Amrani, Hanafi. *Hukum Pidana Pencucian Uang*. Yogyakarta: UII Press, 2015.
- Ardiano, Chandra, Pujiyono Pujiyono, and Nur Rochaeti. "Analisis Yuridis Kriminologis Penggunaan Mata Uang Elektronik Bitcoin Sebagai Sarana Tindak Pidana Pencucian Uang." *Diponegoro Law Journal* 11, no. 1 (2022): 11.
- Bank Indonesia Regulation No. 18/40/2016 concerning Implementation of Payment Transaction Processing.
- Bank Indonesia Regulation No. 19/12/PBI/2017 concerning Implementation of Financial Technology.
- CoFTRA Regulation No. 3 of 2020 concerning Technical Provisions for Organizing Physical Trading of Crypto Assets on Futures Exchanges.
- Conway, Joey. *Beginners Guide to Cryptocurrencies*. Personal blog, May 19, 2014. Retrieved from <https://www.joeyconway.com/blog/wp-content/uploads/2014/10/Beginners-Guide-to-Cryptocurrencies-final.pdf>.
- Crosby, Michael, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. "Blockchain technology: Beyond bitcoin." *Applied Innovation* 2, no. 6-10 (2016): 71.
- Kainama, Maria Minerva, Nuswantoro Dwi Warno, and Joko Setiyono. "Pencegahan Dan Penindakan Penggunaan Virtual Currency Sebagai Sarana Kejahatan Pencucian Uang Melalui Dunia Maya (Studi Kasus Liberty Reserve)." *Diponegoro Law Journal* 6, no. 1 (2017): 1-13.
- Krisnamurti, Hana. "Pembuktian Tindak Pidana Pencucian Uang." *Wacana Paramarta: Jurnal Ilmu Hukum* 14. 1 (2015).
- Kristiana, Yudi. *Pemberantasan tindak pidana pencucian uang: Perspektif hukum progresif*. Yogyakarta: Thafa Media, 2015.
- Lee, David Kuo Chuen, and Linda Low. *Inclusive FinTech: Blockchain, Cryptocurrency and ICO*. Singapore: World Scientific Publishing Co. Pte. Ltd., 2018.
- McJohn, Stephen M., and Ian McJohn. "The Commercial Law of Bitcoin and Blockchain Transactions." *Uniform Commercial Code Law Journal, Forthcoming, Suffolk University Law School Research Paper* 16-13 (2016).
- Merdeka. *Kronologi Terkuaknya Kasus Korupsi Asabri Terbesar Sepanjang Sejarah Indonesia*. Feb 7, 2021. Retrieved from <https://www.merdeka.com/uang/kronologi-terkuaknya-kasus-korupsi-asabri-terbesar-sepanjang-sejarah-indonesia.html>.
- Nurbaiti, Siti. "Kedudukan Hukum Bitcoin Sebagai Mata Uang Virtual Di Indonesia Berdasarkan Undang-Undang Nomor 7 Tahun 2011 Tentang Mata Uang." *Jurnal Hukum Adigama* 1, no. 1 (2018): 1403-1428.
- Parwoto, Adi, Evi Deliana, and Ferawati Ferawati. "Analisis Yuridis Penggunaan Mata Uang Virtual (Bitcoin) Sebagai Sarana Tindak Pidana Pencucian Uang (Money Laundering)." *Jurnal Online Mahasiswa (JOM) Bidang Ilmu Hukum* 6, no. 2 (2019): 1-15.
- Prayogo, Galang, and Yulia Chornous. "Conceptualization of Future Cryptocurrency Laws in Indonesia and Ukraine." *Lex Publica* 7, no. 2 (2020): 56-68.
- Putra, Ade Riyanda Prasetya. "Problematisasi Analisis Ekonomi Terhadap Hukum Tindak Pidana Pencucian Uang." *Lex Renaissance* 4, no. 2 (2019): 303-316.
- Regulation of the Minister of Trade (Permendag) No. 99 of 2018 concerning General Policy for Organizing Crypto Asset Futures Trading.

- Rennock, Michael JW, Alan Cohn, and Jared R. Butcher. "Blockchain technology and regulatory investigations." *Practical Law Litigation* 1 (2018): 35-44.
- Reuters. *Brazil police raids gang allegedly using crypto to launder illegal gold mining*. July 8, 2022. Retrieved from <https://www.reuters.com/world/americas/brazil-police-raids-gang-allegedly-using-crypto-launder-illegal-gold-mining-2022-07-07/>.
- Sam, Y. A. B. L., Messy Rachel Mariana Hutapea, and Suyudi Setiawan. "Legalitas Cryptocurrency dalam Tindak Pidana Kejahatan Pencucian Uang." *Jurnal Ilmu Hukum* 18, no. 1 (2022): 108-120.
- Saragih, Abraham. "Bitcoin dalam Perspektif Kejahatan Siber: Analisis Kriminologi berbasis posmodern." *Jurnal Kriminologi Indonesia* 15, no. 1 (2020).
- Supramono, Gatot. *Hukum Uang di Indonesia*. Bekasi: Gramata Publishing, 2014.,
- Trisakti, Anton Jaksa, and Eko Soponyono. "Upaya Pencegahan Tindak Pidana Pencucian Uang Dalam Bentuk Uang Kripto (Bitcoin) Menggunakan Prinsip Kehati-Hatian Perbankan." *Jurnal Belo* 7, no. 1 (2021): 37-54.
- Utami, Suci. "Tindak Pidana Pencucian Uang Terhadap Uang Virtual Money Laundering on Virtual Money." *Al-Adl: Jurnal Hukum* 13, no. 1 (2021): 1-27.
- Vranken, Harald. "Sustainability of bitcoin and blockchains." *Current opinion in environmental sustainability* 28 (2017): 1-9.
- Wijaya, Dima Ankaa, and Oscar Darmawan. *Blockchain Dari Bitcoin Untuk Dunia*. Jakarta: Jasakom, 2017.
- Wijaya, Dimaz Ankaa. *Mengenal Bitcoin & Cryptocurrency*. Medan: Puspantara, 2016.
- Wijaya, Dimaz Ankaa. *Bitcoin Tingkat Lanjut*. Medan: Puspantara, 2016.
- Wijaya, Firda Nur Amalina. "Bitcoin sebagai digital asset dalam transaksi elektronik di Indonesia (studi pada PT. Indodax Nasional Indonesia)." Master thesis, Universitas Airlangga, 2019.