Unraveling the Vulnerabilities of Abuse and Enforcement of

DIGITAL CURRENCY Related to CRIMINAL OFFENSES

Unraveling the Vulnerabilities of Abuse and Enforcement of Digital Currency Related to Criminal Offenses

Writers : Alia Yofira Karunian
Muhammad Tanziel Aziezi
Seira Tamara Herlambang

Reviewer : Mawa Kresna

Editor : Yassar Aulia
Egi Primayogha

Indonesia Corruption Watch 2024

I.

INTRODUCTION

Technology is rapidly evolving, resulting in the emergence of a variety of new digital innovations. This technological novelty is also occurring in the financial and banking sectors, as economic agents' transaction behaviors shift to digital. One example is the use of cryptocurrencies.

Cryptocurrency is a digital currency that uses cryptographic technology to secure transactions. This cryptography ensures that cryptocurrencies cannot be counterfeited or used multiple times, allowing their owners to avoid potential fraud.[1] The technological support known as blockchain, an integral element of cryptocurrency, also guarantees the security of online transactions even without the involvement of third parties. Many countries have also adopted the use of cryptocurrency as an alternative for cashless transactions, such as cross-border money transfers.[2] Several countries, including the Netherlands, the United Kingdom, Germany, Japan, the United States, and Switzerland, have officially recognized and legitimized the use of cryptocurrency as currency.[3]

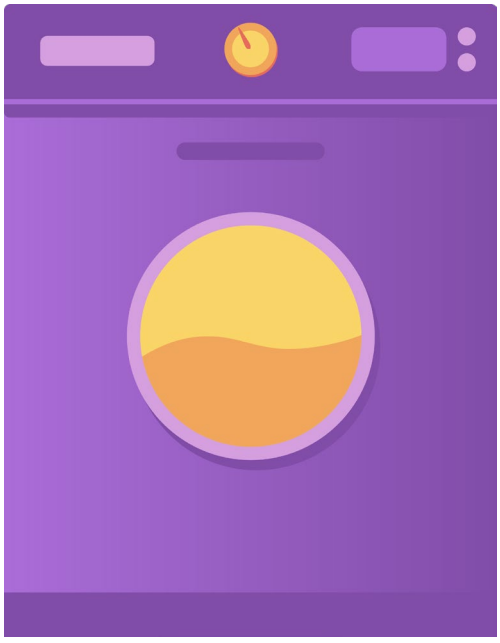
Enthusiasm for the use of crypto continues to increase year by year. On a global scale, the number of crypto users as of November 2023 reached 420 million people with a market capitalization value of US$1.41 trillion.[4] Meanwhile, the Commodity Futures Trading Regulatory Agency (Bappebti) reported that since February 2021, the number of Indonesian users has increased by an average of 437.9 thousand customers per month.[5] The latest data shows that the number of crypto investors in Indonesia reached 19.75 million people in March 2024.[6] In line with the increasing number of users, the value of cryptocurrency transactions has also experienced significant growth. In the period from January to March 2024 alone, the value of cryptocurrency transactions in Indonesia reached Rp158.84 trillion.[7] The amount is even 4 times higher than the transaction value in the same month period in 2023.[8]

---

[1]Dini Diah, "Mengenal Aset Kirpto: Pengertian, Kekurangan, dan Kelebihannya", *Tempo*, 25 July 2023, https://koran.tempo.co/read/ekonomi-dan-bisnis/483403/mengenal-aset-kripto-pengertian-kekurangan-dan-kelebihannya.
[2]Antonius Purwanto, "Mata Uang Kripto: dari Sejarah Awal hingga Regulasi di Indonesia", *Kompaspedia*, 7 January 2022, https://kompaspedia.kompas.id/baca/paparan-topik/mata-uang-kripto-dari-sejarah-awal-hingga-regulasi-di-indonesia.
[3]Muh Afdal Yanuar, "Risiko dan Posibilitas Penyalahgunaan Aset Kripto dalam Kejahatan Pencucian Uang", *Majalah Hukum Nasional Vol. 52, No. 2,* (2022): 170. https://doi.org/10.33331/mhn.v52i2.170.
[4]Kiki Safitri, Aprilia Ika, "Jumlah Investor Kripto di Indonesia Masuk 7 Besar Dunia", *Kompas*, 22 December 2023, https://money.kompas.com/read/2023/12/22/170000726/jumlah-investor-kripto-di-indonesia-masuk-7-besar-dunia.
[5]Kementerian Perdagangan RI, "Bappebti Catat Pelanggan Aset Kripto Tembus 18,25 Juta", 18 December 2023, https://www.kemendag.go.id/berita/pojok-media/bappebti-catat-pelanggan-aset-kripto-tembus-1825-juta
[6]"Potensi Pasar Menjanjkan, Transaksi Kripto di Indonesia meningkat", *Kontan*, 14 May 2024, https://investasi.kontan.co.id/news/potensi-pasar-menjanjikan-transaksi-kripto-di-indonesia-meningkat
[7]Aulia damayanti, "OJK Catat Transaksi Kripto Naik Hampir Rp 70 T dalam Sebulan", *Detik*, 13 May 2024, https://finance.detik.com/fintech/d-7337892/ojk-catat-transaksi-kripto-naik-hampir-rp-70-t-dalam-sebulan.
[8]*Ibid*

Although cryptocurrencies are equipped with a high level of security to protect their users, cryptocurrencies as a commodity do not come without risks. Crypto assets also have a high vulnerability to being misused. This is because transactions through cryptocurrencies can increase anonymity, thereby hindering the detection of criminal activities by law enforcement.[9] This characteristic complicates the tracking of the actual owners of cryptocurrency assets.[10] This gap provides an opportunity for criminals to hide or disguise the assets obtained through their crimes.

This vulnerability is exemplified by data on money laundering through cryptocurrency at the global level, which is quite high, with US$8.6 billion in 2021. When the entire period from 2017 to 2021 was considered, the total value reached US$33 billion.[11] In Indonesia, several cases related to alleged money laundering through crypto have also emerged. For example, the corruption case involving PT Asuransi Sosial Angkatan Bersenjata Republik Indonesia (ASABRI), where the proceeds of the corruption were allegedly used by the perpetrators to purchase crypto assets. Similar to the PT Asabri case, there is also a money laundering case worth tens of billions by former employees of the Directorate General of Taxes at the Ministry of Finance, part of which was transacted to purchase cryptocurrency in the form of Bitcoin.[12]



US$33 billion

The total amount of money laundered through cryptocurrency from 2017 to 2021

US$8.6 billion

Data on cryptocurrency-related money laundering in 2021

[9]Muh Afdal Yanuar, *op.cit.*, p. 174.
[10]*Ibid*
[11]James Thorpe, "US$ 8.6 Billion Worth of Cryptocurrency Laundered by Cybercriminals in 2021", *International Security Journal*, 21 February 2022, https://internationalsecurityjournal.com/cryptocurrency-laundered-in-2021/
[12]"Rafael Cuci Uang Miliaran Pakai Bitcoin, Ini kata PPATK!", *CNBC Indonesia*, 12 May 2023, https://www.cnbcindonesia.com/news/20230512113504-4-436827/rafael-cuci-uang-miliaran-pakai-bitcoin-ini-kata-ppatk

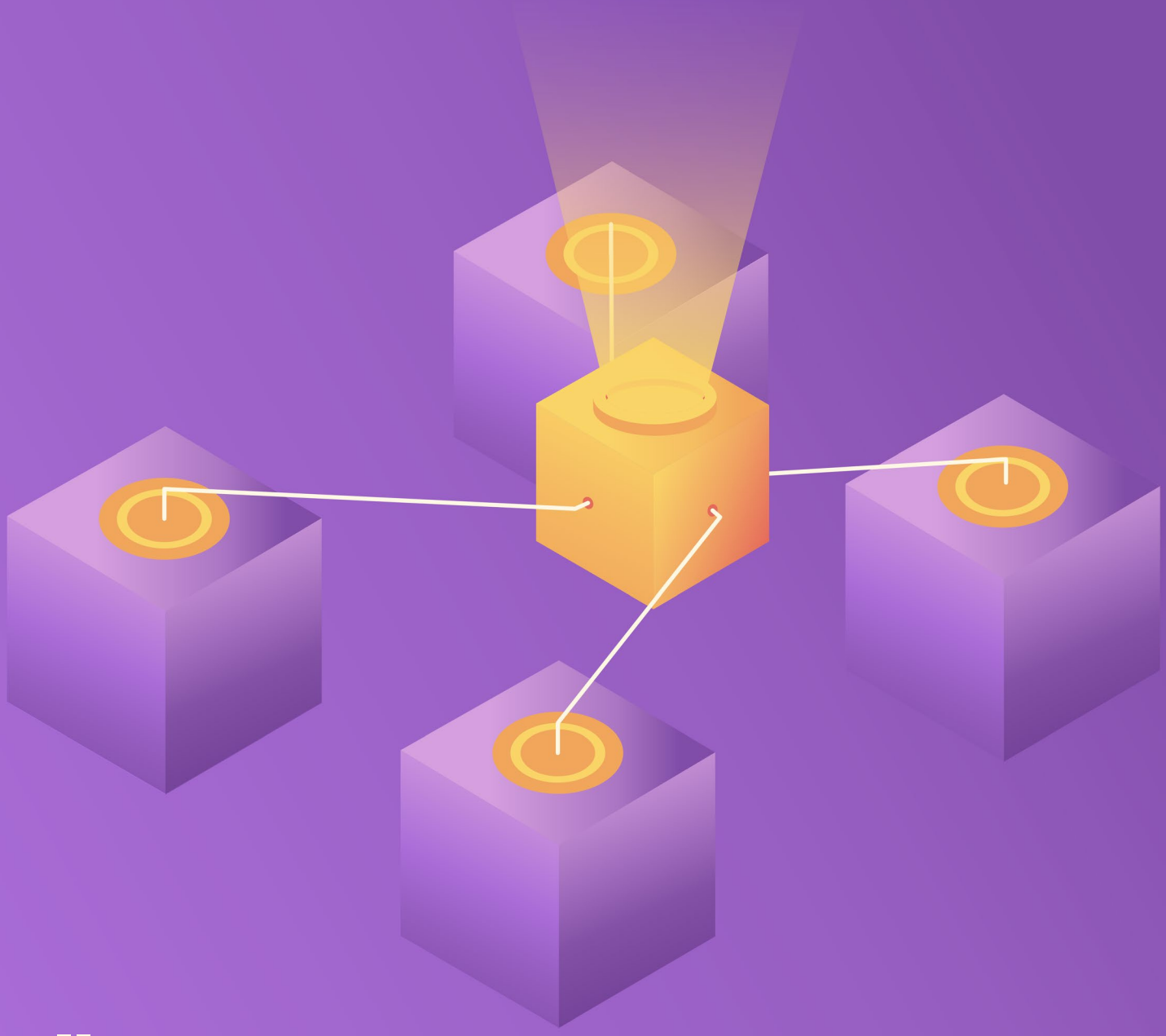
Money laundering is the process of concealing illegally obtained assets in order to make them appear legal. Cryptocurrency's unique characteristics have the potential to be used as a tool for concealing assets obtained illegally. Corruption, and drug trafficking, are common high-risk source crimes in cryptocurrency misuse.[13] Not only that, cryptocurrency assets also allow for concealing the proceeds of other crimes such as environmental crimes. Moreover, the Financial Transaction Reports and Analysis Center (PPATK) in mid-2023 also discovered suspected illegal fund flows, including money laundering related to environmental crimes, amounting to a staggering Rp20 trillion.[14]

Several of the explanations above emphasize the importance of further investigation into the potential misuse of cryptocurrency in concealing assets from criminal activity, as well as the measures that can be taken to combat it. This report will examine the current state of regulations, preventive measures, and law enforcement actions involving cryptocurrency. This report will also address the challenges and opportunities for improving current prevention and enforcement efforts.

---

[13]Muh Afdal Yanuar, *loc.cit.*

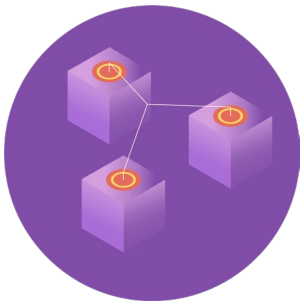
[14]Rahel Narda Chaterine, dan Sabrina Asril, "PPATK: Pencucian Uang Terkait Kejahatan Lingkungan Sampai Rp20 Triliun", *Kompas*, 27 June 2023, https://nasional.kompas.com/read/2023/06/27/16081621/ppatk-pencucian-uang-terkait-kejahatan-lingkungan-sampai-rp-20-triliun



II.

UNDERSTANDING BLOCKCHAIN TECHNOLOGY AND CRYPTOCURRENCY

A. *Blockchain*



The origin of the name blockchain technology is related to how this technology stores transaction data, namely in a block that is linked together to form a chain.[15] The core idea of blockchain first emerged in the late 1980s and early 1990s, as a protocol called the "Paxos Protocol" conceived by Leslie Lamport.[16] In 2008, blockchain began to be widely recognized as the technology underlying cryptocurrency, Bitcoin, which was conceived by someone (or a group of people) known by the pseudonym Satoshi Nakamoto.[17] Satoshi envisioned that in the future, money transactions between parties would be recorded in a shared ledger, managed by computers spread across the world (a network of "nodes").[18]

In line with Satoshi's vision, Tran and Krishnamachari (2022) then technically defined blockchain as "a decentralized computing system consisting of five components: a decentralized network, mathematical cryptography, distributed consensus, a transaction ledger, and smart contracts."[19] As for further explanations regarding the five components, among others:

Table 1: Components of Blockchain Technology

Blockchain Components	Description
Decentralized Network	*Blockchain is a decentralized computer network (referred to as nodes), which then becomes a computational resource to help store and process transactions.*

[15]Duc A. Tran, My T. Thai, and Bhaskar Krishnamachari, eds., *Handbook on Blockchain*, vol. 194, Springer Optimization and Its Applications (Cham: Springer International Publishing, 2022), 4, https://doi.org/10.1007/978-3-031-07535-3.
[16]Leslie Lamport, "The Part-Time Parliament," ACM Transactions on Computer Systems 16, no. 2 (May 1, 1998): 133–69, https://doi.org/10.1145/279227.279229.
[17]Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," accessed February 14, 2023, https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf.
[18]Valentina Gatteschi, Fabrizio Lamberti, and Claudio Demartini, "Technology of Smart Contracts," in *The Cambridge Handbook of Smart Contracts*, Blockchain Technology and Digital Platforms, ed. Larry A. DiMatteo, Michel Cannarsa, and Cristina Poncibò, 1st ed. (Cambridge University Press, 2019), 39, https://doi.org/10.1017/9781108592239.003.
[19]Tran, Thai, and Krishnamachari, *Handbook on Blockchain*, 194:6.

Blockchain Components	Description
Mathematical Cryptography	*Blockchain uses cryptographic methods that also serve to prove that mathematically, blockchain functions as it should. Furthermore, blockchain uses cryptographic hashes to link data blocks in a chain to prevent data alteration after the recording of new data blocks in the blockchain system (immutability).*
Distributed Consensus	To determine the validity of a transaction, there is no central authority that decides. On the contrary, the decision is made based on the consensus reached among the participating network nodes. Currently, there are two types of consensus mechanisms commonly used in blockchain systems, namely proof-of-work (POW) and proof-of-stake (POS).
Transaction Ledger	*Blockchain is a digital ledger that stores transactions chronologically in blocks that are added to existing data (append-only). This is the data structure that underlies how the ledger for almost all blockchain networks operates.*
Smart Contract	Applications that use blockchain technology are implemented as smart contracts, a term coined by Nick Szabo in 1994.[20] Smart contracts differ from traditional contracts because their execution is automatic, without human intervention.

(Source: Handbook on Blockchain, 2022)

[20]Nick Szabo, "Smart Contracts," 1994, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

Furthermore, Tran and Krishnamachari (2022) also highlighted at least three characteristics that make blockchain technology distinct, namely "secure (no possibility of data loss or alteration), transparent (easy verification and tracing), and trustless (transaction trust without intermediaries)."[21]

Based on the permission restrictions for nodes to add data to the blockchain system, blockchain technology can be classified into two types, namely Permissionless Blockchain (nodes do not require permission to participate) and Permissioned Blockchain (nodes require permission to participate).[22] Furthermore, based on who can access and view the shared blockchain ledger, the blockchain can also be categorized as public (open for anyone to view) or private (accessible only to network node participants who have been granted prior approval).[23]

Blockchain technology is touted to be superior compared to other technologies that adopt a centralized approach, particularly in four crucial aspects: trust, security, privacy, and transparency.[24] Nevertheless, there are quite a few parties voicing concerns about blockchain technology in these four crucial aspects. Suripeddi and Purandare (2021), for example, both underline how the negative impact of blockchain utilization affects the right to privacy, particularly concerning the protection of blockchain users' personal data.[25] In addition, the study conducted by Tuyisenge (2021) also found that blockchain technology is not free from digital security attacks. Tuyisenge identified that 51% of security attacks result in double spending and unfair income, while attacks on software wallets lead to unauthorized code execution, denial of service, and leakage of users' private keys.[26]

Another aspect that has also been highlighted regarding the utilization of blockchain technology is its impact on the environment, particularly concerning the energy consumption required to support blockchain technology. In a blockchain system that uses the POW consensus mechanism, for example, the mining process consumes electricity equivalent to-

---

[21]Tran, Thai, and Krishnamachari, *Handbook on Blockchain*, 194:6.
[22]Harish Natarajan, Solvej Krause, and Helen Gradstein, "Distributed Ledger Technology (DLT) and Blockchain: FinTech Note No. 1" (World Bank, 2017), IV, https://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf.
[23]Natarajan, Krause, and Gradstein, IV.
[24]Tran, Thai, and Krishnamachari, *Handbook on Blockchain*, 194:4.
[25]Mani Karthik Suhas Suripeddi and Pradnya Purandare, "Blockchain and GDPR – A Study on Compatibility Issues of the Distributed Ledger Technology with GDPR Data Processing," J*ournal of Physics: Conference Series* 1964, no. 4 (July 2021): 11, https://doi.org/10.1088/1742-6596/1964/4/042005.
[26]Marie Jeanne Tuyisenge, "Blockchain Technology Security Concerns: Literature Review" (Sweden, Uppsala Universitet, 2021), 41, https://www.diva-portal.org/smash/get/diva2:1571072/FULLTEXT01.pdf.

the annual electricity consumption of the country of Switzerland.[27] Specifically, various studies that specifically examine the environmental impact of the Bitcoin mining process (one type of cryptocurrency) heavily rely on fossil fuels.[28] As much as 67% of the electricity used for Bitcoin mining from 2020 to 2021 was generated from fossil energy sources. From the fossil fuel usage figures, coal dominated the electricity supply used for Bitcoin mining, accounting for 45% globally during the same period.[29]

On the other hand, various efforts have been made to mitigate the environmental impact of the Blockchain mining process. A study conducted in 2023 identified at least 23 blockchain networks that consume significantly less power and produce less carbon dioxide emissions compared to the Bitcoin network.[30] Nevertheless, Bitcoin still remains the dominant type of blockchain in the cryptocurrency market in Indonesia. In 2024, Bappebti recorded that Bitcoin dominated more than half of the total cryptocurrency market capitalization in Indonesia.

The extensive use and dependence on energy, particularly from coal, in the mining process of blockchain networks, especially Bitcoin, has the potential to cause environmental damage as an unavoidable consequence. Therefore, when analyzing the cost efficiency of blockchain technology, it is also important to consider the environmental impact as a determining factor.

---

[27]Sherman Lee, "Bitcoin's Energy Consumption Can Power An Entire Country -- But EOS Is Trying To Fix That," *Forbes*, 19 April 2018
https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/.

[28]"UN Study Reveals the Hidden Environmental Impacts of Bitcoin: Carbon is Not the Only Harmful By-product", *United Nations University* (Press Release), 24 October 2023,
https://unu.edu/press-release/un-study-reveals-hidden-environmental-impacts-bitcoin-carbon-not-only-harmful-product

[29]*ibid*

[30]Yehia Ibrahim Alzoubi and Alok Mishra, 'Green Blockchain – A Move towards Sustainability' (2023) 430 Journal of Cleaner Production 139541.

[31]Pusat Data dan Sistem Informasi Kementerian Perdagangan Indonesia, "Bappebti Targetkan Transaksi Kripto Rp800 Triliun pada 2024", *Kementerian Perdagangan Republik Indonesia*, 3 February 2024,
https://www.kemendag.go.id/berita/pojok-media/bappebti-targetkan-transaksi-kripto-rp800-triliun-pada-2024.

B. Cryptocurrency: 101

In 2023, Indonesia ranked 6th in the world for the highest cryptocurrency ownership. This relatively high ranking was achieved by Indonesia, despite a sharp decline in cryptocurrency transaction volume in Indonesia by 63% in 2022.[33] Despite the global decline in the cryptocurrency market,[34] Chainalysis, a company focused on blockchain analysis and crypto investigation services, noted that there has been an increase in the volume of dark crypto transactions for two consecutive years, reaching an all-time high of US$20.6 billion in 2022.[35] Furthermore, Chainalysis also found that the amount of cryptocurrency resulting from money laundering increased by 68% in 2022.[36] The Indonesian government has long identified the use of cryptocurrency, Bitcoin, as a current form of threat in money laundering crimes since 2015.[37]

So what is cryptocurrency, often referred to as cryptocurrency? A study conducted by the European Parliament shows that in the context of regulation, there is no agreed-upon definition of cryptocurrency. Various banking and financial institutions worldwide categorize cryptocurrency as part of digital or virtual currency.[38] The European Parliament defines cryptocurrency as "a representation of digital value that (i) is intended as a peer-to-peer (P2P) alternative to government-issued legal tender, (ii) is used as a medium of exchange for general purposes (regardless of any central banking institution), (iii) is secured by mechanisms called cryptography, and (iv) can be converted into legal tender and vice versa."[39] In the same study, there are several actors that can be identified in the cryptocurrency trading ecosystem. As for those actors, inter alia:[40]

---

[32]"The State of Crypto & NFTs in 2023," DataReportal – Global Digital Insights, 28 January 2023, https://datareportal.com/reports/digital-2023-deep-dive-blockchains-roadblocks.

[33]Shenna Peter, "Indonesian Crypto Exchanges Blame Dramatic Drop in Trading Volumes Partly on High Taxes," 17 January 2024, https://www.coindesk.com/policy/2024/01/17/indonesian-crypto-exchanges-blame-dramatic-drop-in-trading-volumes-partly-on-high-taxes/.

[34]"The State of Crypto & NFTs in 2023."

[35]"The 2023 Crypto Crime Report" (Chainalysis, February 2023), 5, https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf.

[36]"The 2023 Crypto Crime Report," 43.

[37]"Penilaian Risiko Indonesia Terhadap Tindak Pidana Pencucian Uang" (Tim National Risk Assessment (NRA) Indonesia, 2015), 56, https://www.ppatk.go.id/backend/assets/uploads/20170911141103.pdf.

[38]Robby Houben and Alexander Snyers, "Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion" (European Parliament, July 2018), 20–23, https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2018)619024.

[39]Houben and Snyers, 23.

[40]Houben and Snyers, 25–28.

Table 2: Actors in the Cryptocurrency Ecosystem

Actors	Role
User	Individuals or legal entities who obtain coins to use them for (i) purchasing real or virtual goods or services (from a specific group of merchants), (ii) making Peer-to-Peer payments, or (iii) holding them for investment purposes. Every user in the blockchain network has two keys: (i) a private key, which is used to create a digital signature in a transaction, and (ii) a public key, which is known by all other actors in the blockchain network.[41]
Miner	Miners consist of users or other parties who seek to profit from the cryptocurrency mining process to then exchange it for fiat currency. Miners participate in the transaction validation process within the blockchain system by solving cryptographic puzzles. This mining process is specifically related to cryptocurrencies that use the POW consensus mechanism.
Cryptocurrency Exchanges	A cryptocurrency exchange is a legal entity that offers cryptocurrency exchange services to users, usually for a certain fee. The services offered can include cryptocurrency exchange services to sell their coins for fiat currency, or conversely, to buy new coins with fiat currency.

[41]Houben and Snyers, 16.

Actors	Role
Trading Platforms	Cryptocurrency trading platforms are marketplaces that connect cryptocurrency users with each other so they can buy and sell directly (for example, an "eBay" for cryptocurrency users).
Wallet Providers	A cryptocurrency wallet service provider is an entity that offers digital wallet services to cryptocurrency users, allowing them to easily store and transfer coins.
Coin Inventors	Coin inventios are individuals or organizations that develop the technical foundation of cryptocurrency and determine the initial rules for its use. In some cases, the identity of the coin creators is known (for example, Ethereum, Ripple, Litecoin, Cardano), but in other cases, the identity of the cryptocurrency creators is unknown (for example, Bitcoin and Monero).
Coin Offerors	A coin offeror is an individual or organization that offers cryptocurrency coins to users after the release of the coin, either for a certain fee or for free. Coin distributors can also be the same party as the Coin Creators, or they can be separate individuals or organizations.

Source: *Cryptocurrencies and Blockchain*, 2018

Cryptocurrency exchanges, as places where users can exchange cryptocurrency coins for fiat currency, have become the largest recipients of illegal cryptocurrency.[42] Besides cryptocurrency exchanges, another party that also facilitates money laundering of cryptocurrencies is wallet providers. In a study conducted by Transparency International Russia (2023), it was found that there are intermediaries on the dark web offering money-

[42] "The 2023 Crypto Crime Report," 43.

mule accounts on Wirex for a certain fee.[43] *These money mule accounts are generally registered in the names of citizens or refugees who have residence permits in countries such as Ukraine, Latvia, Estonia, Poland, the Czech Republic, Bulgaria, and Spain.*[44] *The sellers of these money mule accounts also agree to sell accounts in large quantities, which then opens up the possibility of smurfing (a money laundering practice by breaking down large amounts of money into several smaller transactions to avoid money laundering scrutiny).*[45]

Therefore, efforts to regulate cryptocurrency transactions should target high-risk actors, such as:

Cryptocurrency Exchanges

Trading Platforms

Wallet Providers

In practice, a single company can play dual roles and offer more than one of the three services mentioned above. For example, the physical crypto asset trader, INDODAX, also offers exchange services (cryptocurrency exchanges) and wallet services (wallet providers) for cryptocurrencies.[46] *In addition, it is important to further understand the various business models of wallet providers, which greatly impact efforts to combat crimes involving cryptocurrencies. Wallet providers are essentially divided based on how they store the user's keys (public and private) used to validate cryptocurrency transactions. In general, wallet providers are divided into the following groups:*

---

[43]"Anonymity For Sale: The Thriving Black Market Of Crypto-To-Fiat Mules" (Transparency International Russia, 2023), 43, https://ti-russia.org/wp-content/uploads/2023/10/epaycrypto_.pdf.
[44]"Anonymity For Sale: The Thriving Black Market Of Crypto-To-Fiat Mules," 29.
[45]"Anonymity For Sale: The Thriving Black Market Of Crypto-To-Fiat Mules," 30.
[46]indodax academy, "Kumpulan: Cara Trading Crypto," *Belajar Jual Bitcoin Beli Bitcoin | Indodax Academy (blog)*, July 27, 2022, https://indodax.com/academy/trading-di-indodax/.

1 Based on whether the user has full control over the private key

Based on these criteria, wallet providers are divided into two categories: non-custodial (also known as 'unhosted wallet') and custodial wallet (also known as 'hosted wallet').[47] The differences in characteristics between the two are as follows:[48]

Table 3: The difference between Custodial and Non-Custodial Wallet

Custodial Wallet	Non-Custodial Wallet
Custodial wallet users do not have full control	Non-custodial wallet users have full control
The user's private key is stored by a third party (centralized)	*Private key is stored only by the user (decentralized)*
Private key is available online	*Private key is available online and offline*

2 Based on whether the wallet is connected to the internet or not

Based on this criterion, wallet providers are divided into two categories: hot and cold wallets. The differences in characteristics between the two are as follows:[49]

Tabel 4: Perbedaan *Hot* dan *Cold Wallet*

Hot Wallet	Cold Wallet
Connected to the internet continuously	Not continuously connected to the internet
Virtual Wallet	Virtual and Physical Wallet
Type: Desktop, Mobile, or Hybrid (a combination of both)	Type: Hardware (e.g., USB) or Paper (e.g., QR code)

[47] "Policy Recommendations for Crypto and Digital Asset Markets" (International Organization of Securities Commissions, November 2023), 45, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf.
[48] Pamela, "Ini Perbedaan Custodial Wallet Dan Non-Custodial Wallet Pada Crypto!," *Ajaib Kripto (blog)*, December 25, 2022, https://kripto.ajaib.co.id/perbedaan-custodial-wallet-dan-non-custodial-wallet/.
[49] Aldo Pradianto, "Hot Wallet: Jenis, Kelebihan, & Perbedaan dengan Cold Wallet," *Belajar Jual Bitcoin Beli Bitcoin | Indodax Academy (blog)*, October 12, 2023, https://indodax.com/academy/hot-wallet/.

III.

REGULATIONS AND PRACTICES FOR PREVENTING AND COMBATING CRIMES INVOLVING DIGITAL CURRENCY

A. Overview of Crimes Involving Digital Currency

In recent years, digital currencies have evolved into one of the payment mechanisms built on the system or software protocol of the digital currency itself. This payment mechanism seeks to provide a new method for transferring a certain value over the internet. However, at the same time, digital currency payment products and services pose risks of money laundering, terrorism financing, and other crimes that must be identified and mitigated.[50]

Currently, criminals are increasingly exploiting digital assets or currencies as the use of digital currencies, particularly cryptocurrencies, becomes more widespread and rapidly diversified. In this regard, the U.S. Department of Justice (DOJ) in the document The Cryptocurrency Enforcement Framework[51] categorizing the forms of digital currency relationships with crime as follows:[52]

#1

Digital currency as a means of payment or a way to facilitate the commission of crimes

In some cases, it was found that digital currencies were used to buy and sell illegal drugs, to spread advertisements and promote human trafficking, becoming a preferred method and collection method for ransomware payments.[53] and other digital extortion activities, to commit fraud and theft against consumers and investors, and to finance threats to national security, including fundraising for terrorist activities.

[50]The Financial Action Task Force (FATF), *Guidance for a Risk-based Approach: Virtual Currencies*, (Paris: FATF, 2015), hal. 3.
[51]The Cryptocurrency Enforcement Framework is a document that explains the legal procedures available to prosecute the illegal use of digital currencies, outlines the profiles, roles, and responsibilities of government agencies in the field of digital assets, and describes strategies to address emerging threats to the security and effective operation of the digital currency market. See U.S. Department of Justice, . See *U.S. Department of Justice, The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067: The Role of Law Enforcement In Detecting, Investigating, and Prosecuting Criminal Activity Related To Digital Assets,* (Washington: U.S. Department of Justice, 2022), p. 14.
[52]Ibid., p. 4 – 9.
[53]Ransomware is a type of malware or virus that is inserted by the perpetrator into the victim's computer system and locks the data within the computer, where the ransomware perpetrator will demand a ransom from the victim if they want to unlock the locked data. Generally, the ransom does not use commonly used currency, but rather virtual currency Bitcoin. In addition, this virus can also lock the entire system, making the only way to regain access to the computer by paying the ransom demanded. See the Telecommunications and Information Accessibility Agency, , "Ciri-Ciri Komputer Terinfeksi Ransomware & Cara Mengatasinya",
https://www.baktikominfo.id/id/informasi/pengetahuan/ciri-ciri_komputer_terinfeksi_ransomware_cara_mengatasinya-750, accesses on Thursday, 15 February 2024.

This is done by criminals by exploiting the anonymity of digital currencies, thereby concealing the true identities of the perpetrators. In fact, in 2021, the Federal Bureau of Investigation (FBI) of the United States received 3,729 complaints related to ransomware through the Internet Crime Complaint Center, with losses amounting to more than US$49.2 million;

#2

The use of digital currency as a means to conceal illicit financial activities

Besides being a means of payment for a crime, in some other cases, criminals also use digital currencies to commit money laundering and facilitate tax evasion. In addition to exploiting the nature of anonymity, these criminals also rely on increasingly sophisticated obfuscation techniques, such as complex and rapid transactions, "chain hopping" by converting funds from one digital currency to another, and other actions designed to complicate tracing and render the digital currency unrecoverable. These crimes have become easier to commit because many digital currency platforms and exchanges do not strive to comply with anti-money laundering regulations, such as "Know Your Customer" (KYC) requirements, or operate in jurisdictions that lack anti-money laundering rules and funding eradication requirements in line with international standards.

#3

Crimes that involve or affect the digital currency ecosystem

As interest in the use of digital currencies has increased, creating significant market opportunities, criminals targeting the digital currency ecosystem have also emerged, such as digital currency theft, fraud with proceeds in digital currency, and crimes involving specialized technology like crypto jacking, which is the unauthorized use of someone else's computer to mine digital currency. According to estimates from a blockchain analysis company, more than US$3.2 billion worth of digital currency was stolen, both from individuals and-

digital currency services in 2021. An example of a digital currency theft case is the Lazarus Group case in March 2022, which stole digital currency worth more than US$600 million from an online gaming platform, and the digital currency theft worth US$8 billion carried out by FTX cryptocurrency exchange founder Sam Bankman-Fried in November 2022.[54]

For money laundering cases, the involvement of digital currencies in such crimes has occurred in several instances, including:

1. In England, the London Metropolitan Police successfully seized cryptocurrency worth £180,000,000 in July 2021, and the U.K.'s National Crime Agency (NCA) confiscated digital currency worth £26,900,000 between April 1, 2021, and March 31, 2022. The two seizure cases are suspected to be related to money laundering crimes;[55]

2. The "Silk Road" case in the United States in 2013-2014. In that case, the US Department of Justice successfully seized the Silk Road website (a hidden website designed to allow its users to conduct transactions involving drugs, weapons, stolen identity information, computer hacking, and money laundering) and confiscated 173,991 Bitcoins worth £33,600,000 from the seized computer devices on Silk Road;[56]

3. The case of the cryptocurrency exchange company Binance in the United States, which was charged with violating U.S. anti-money laundering laws for processing financial transactions related to various criminal activities. In that case, Binance founder Changpeng Zhao pleaded guilty to the crime and was sentenced to 4 months in prison, fined US$ 50 million, and ordered by the court to resign from his position as CEO of Binance. The court also imposed a fine of US$ 4.3 billion on Binance as a company.[57]

---

[54]Curi Rp. 125 T Duit Nasabah, Bandar Kripto ini Dihukum 25 Tahun Penjara", *CNBC Indonesia*, 30 March 2024, https://www.cnbcindonesia.com/tech/20240330071156-37-526656/curi-rp125-t-duit-nasabah-bandar-kripto-ini-dihukum-25-tahun-penjara.

[55]Alessio D. Evangelista, dkk, "*Cryptoasset Seizures and Forfeitures: US and UK Enforcement Overview*", Skadden, 7 September 2022, https://www.skadden.com/insights/publications/2022/09/cryptoasset-seizures-and-forfeitures

[56]FATF, *Guidance for a Risk-based Approach: Virtual Currencies…*, *Op. Cit.*, p. 32-34. Lihat juga U.S. Department of Justice, *The Report of the Attorney General…*, *Op. Cit.*, p. 14

[57]"Binance Tempat Cuci Uang, Raja Kripto Dunia Dijebloskan ke Penjara", *CNBC Indonesia*, 1 May 2024, https://www.cnbcindonesia.com/tech/20240501180513-37-534995/binance-tempat-cuci-uang-raja-kripto-dunia-dijebloskan-ke-penjara.

In response to those crimes, the Financial Action Task Force (FATF)[58] revealing that crimes involving digital currencies occur because the perpetrators can exploit the unique features of digital currencies, such as fast and irreversible transaction settlements, as well as the use of addresses and pseudonyms. This situation is further exacerbated by the growing online market for illegal digital currencies, such as Silk Road and Alphabay, which are often hosted anonymously on the "darknet," a part of the Internet that is not indexed by search engines and requires special software to access. FATF then outlined several factors that make digital currencies potentially risky for use in crimes such as money laundering and terrorist financing, including:[59]

1. The use of digital currency allows for greater anonymity compared to traditional non-cash payment methods. Digital currencies can be traded on the Internet, generally characterized by non-face-to-face customer relationships, and open up opportunities for anonymous funding, namely cash funding or third-party funding through virtual exchanges that do not precisely identify the source of funding. This method also provides the opportunity for anonymous transfers even though the sender and recipient are not adequately identified;

2. The nature of this anonymity further makes digital currencies vulnerable to misuse due to their decentralized trading system, which lacks centralized servers or service providers for digital currencies. For example, in Bitcoin, the Bitcoin address that functions as an account does not have a name or other identification methods, and the Bitcoin protocol does not generate a transaction history record that must be linked to the identity of the parties transacting in the real world. Due to the absence of a centralized server as a supervisory body and the lack of anti-money laundering software to monitor and identify-

---

[58]The Financial Action Task Force (FATF) is an intergovernmental body that functions as a watchdog in the prevention and prosecution of global money laundering and terrorist financing crimes. To do this, the FATF sets international standards aimed at preventing these illegal activities and the harm they cause to society. See FATF's profile at https://www.fatf-gafi.org/en/the-fatf/who-we-are.html , accessed on Thursday, 15 February 2024. Indonesia has been the 40th member of the FATF since October 27, 2023. See Ministry of Finance of the Republic of Indonesia, "Indonesia Resmi Jadi Anggota Penuh FATF, Menkeu: Bawa Dampak Positif bagi Kredibilitas Perekonomian Negara", https://www.kemenkeu.go.id/informasi-publik/publikasi/berita-utama/Indonesia-Resmi-Jadi-Anggota-Penuh-FATF , Accessed on Thursday, 15 February 2024.

[59]FATF, *Guidance for a Risk-based Approach: Virtual Currencies* …, Op. Cit., p. 31-32. Lihat juga The Financial Action Task Force (FATF), *Guidance for a Risk-Based Approach: Virtual Asset and Virtual Asset Service Providers,* (Paris: FATF, 2019), par. 28.

suspicious transaction patterns, law enforcement cannot easily target a single location or central entity (administrator) for investigation or seizure purposes when Bitcoin is misused;

3. Digital currency transactions can be conducted over the internet with a global reach (cross-border). Moreover, digital currency transactions usually involve several entities that are often located in different jurisdictions, including places that do not have adequate anti-money laundering/terrorist financing prevention mechanisms. This causes ambiguity regarding which parties should be responsible for compliance and oversight/enforcement of anti-money laundering/terrorist financing regulations, and makes it difficult for law enforcement and regulators to access digital currency transaction data, especially given the nature of anonymity and decentralization.

The issue of anonymity in digital currency transactions mentioned above is also believed by the European Parliament and the Council of the European Union to increase the potential for the misuse of digital currency for criminal purposes. The European Parliament and the Council of the European Union added that the involvement of entities as exchange services between virtual currencies and fiat currencies, as well as custodial wallet providers, will not fully address the inherent anonymity issue in digital currency transactions. This is because virtual currency transactions can still be conducted anonymously when users transact without the provider. To reduce the risk of that anonymity, the Financial Intelligence Unit (FIU) must be able to obtain information that allows the FIU to link the digital currency address with the identity of the digital currency owner. [60]

B. Environmental Crime and the Involvement of Digital Currency

Referring to the United Nations Environment Programme (UNEP) and INTERPOL, environmental crime is described as illegal activities that harm the environment and aim to benefit individuals, groups, and/or companies from the exploitation, destruction, trade, or theft of natural resources, which include but are not limited to serious crimes-

[60] The European Parliament and the Council of the European Union, *Amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, Regulation (EU) 2023/1114*, Directive (EU) 2018/843, 30 May 2018, par. 9.

and transnational organized crime.[61] Illegal activities in environmental crimes include wildlife crimes, pollution crimes, trade in banned chemicals, illegal fishing and mining, as well as illegal logging.

Currently, environmental crime is at a concerning level. In 2021, environmental crimes even made it into the top three global crimes, with illegal profits reaching US$281 billion.[62] This situation is certainly very concerning, as environmental crimes have implications that not only involve the destruction and scarcity of natural resources, the disruption of human health, but also hinder socio-economic development.[63] Both nature and community life must bear the consequences of environmental crimes. In the context of community life, environmental crimes can benefit armed groups and trigger security conflicts.

Environmental crime has a character similar to drug trafficking and human trafficking. These crimes are committed across national borders and therefore fall into the category of transnational crimes. For example, the execution of exploitation activities, the presence of receivers, and the locations of money laundering from illegal activities are in different countries. In the end, environmental crimes also lead to other crimes such as money laundering and illicit financing.[64] In this aspect, crypto is vulnerable to being used as a medium that facilitates it, as transactions using crypto can be conducted with a wide cross-border reach.

Although no specific cases have been found, the potential misuse of cryptocurrency as a medium for laundering money from environmental crimes still needs to be monitored. This argument is also supported by findings from the Asia Pacific Group-UNODC, which state that information related to payment methods or other means used to facilitate environmental crimes is very limited. In addition to the factor that reports on environmental crimes are incomplete and fragmented, the lack of information on this matter also indicates that the use of instruments allowing for anonymity and complexity in tracking is very likely to be employed.[65] This means that the use of cryptocurrency also has the potential to be used as a medium for channeling assets from environmental crimes.

---

[61]Benjamin Kurylo, "Explainer: What is Environmental Crime?", *Earth.org*, 25 March 2024, https://earth.org/explainer-what-is-environmental-crime/.
[62]Amandra Megarani, "Nilai Kejahatan Lingkungan Rp4.074 Triliun", *Forest Digest*, 1 April 2022, https://www.forestdigest.com/detail/1626/kejahatan-lingkungan
[63]Benjamin Kurylo, *loc.cit.*
[64]Amandra Megarani, *loc.cit.*
[65]Stefano Sigia, "Environmental Crimes and Money Laundering", *Pideeco*, 22 June 2020, https://pideeco.be/articles/environmental-green-crimes-aml-money-laundering/

Not only as a medium of transaction, crypto can also be used to disguise money from environmental crimes through crypto mining funding. Europol data in 2022 showed that cryptocurrency money laundering operations were reported as the highest proportion compared to other illegal uses of cryptocurrency, such as fraud.[66] In this context, the profits from environmental crimes can be used as a source of funding for cryptocurrency mining that produces new digital coins. There is no direct connection between these new coins and criminal activities or their origins, as the process of cryptocurrency mining itself is also legal. After that, the coin can be resold as fiat currency, so the perpetrators ultimately end up with an asset that appears clean, even though it originates from environmental crime.

Based on that possibility, regulations related to digital currencies are needed, particularly those that can support the prevention and enforcement of crimes involving digital currencies. The absence of such regulations poses a significant risk to the overall integrity of the digital currency market. The misuse of digital currencies and their markets for certain crimes can lead to a lack of trust among digital currency users, which can significantly hinder the development of that asset market. This has the potential to result in the loss of opportunities in terms of innovative digital services and the emergence of alternative payment instruments or new sources of funding.[67]

C. Regulations and Common Practices Related to the Prevention and Enforcement of Crimes Involving Digital Currency

In its development, several parties/institutions have issued standards or regulations for handling digital currencies, including in relation to law enforcement against certain crimes involving digital currencies such as money laundering and terrorism financing. One of the widely followed global standards for handling digital currencies is the standards issued by FATF. This institution has issued many regulations related to the handling of money laundering and terrorism financing crimes, which then provide context for these crimes with digital currencies. For example, the FATF document in 2014 that outlines the definitions of terminology in digital currency transactions and the potential involvement of digital currencies-

---

[66]S Elsayed, "Cryptocurrencies, Corruption, and Organised Crime", *U4 Helpdesk Answer*, 2023, accessed from https://www.u4.no/publications/cryptocurrencies-corruption-and-organised-crime.pdf.

[67]The European Parliament and the Council of the European Union, *markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937*, Regulation (EU) 2023/1114, 31 Mei 2023, par. 4 and 5.

currencies in money laundering and terrorist financing crimes.[68]

In general, the regulations for law enforcement related to digital currencies in FATF documents can be divided into two parts, namely rules related to prevention and crime enforcement. The rules related to prevention mainly regulate the transaction systems and the obligations of the parties involved in digital currency transactions to avoid the involvement of digital currencies in money laundering and terrorist financing crimes. Meanwhile, the rules related to enforcement focus more on the authority of law enforcement agencies and the obligations of parties involved in digital currency transactions if there is a crime suspected to involve digital currency. Further explanation regarding these regulations is as follows:

1 Prevention

As mentioned earlier, FATF has acknowledged that there is a risk of money laundering and terrorist financing crimes involving digital currencies and the activities of Virtual Asset Service Providers (VASPs) as parties providing digital currency transaction services. Therefore, FATF urges each country to take preventive measures by identifying, assessing, and understanding the risks of such crimes in digital currency transactions, at least by considering the types of services, products, or transactions involved; the risk profile of service users; geographical factors; and the types of digital currencies being exchanged. Not only must this be done directly by the state, but the state must also require VASPs and other obligated entities involved in financial activities or operations or providing digital currency services to identify, assess, and take effective actions to mitigate the risks of money laundering and terrorist financing in their service execution.[69]

In general, FATF formulates measures to prevent crimes involving digital currencies in its recommendations number 15 and 16 in the document on the prevention and suppression of money laundering and terrorist financing. FATF also formulated interpretative notes for each of these recommendations to make them easier for each country to implement. Some important regulations according to each recommendation and interpretative note are as follows:[70]

---

[68]Lihat The Financial Action Task Force (FATF), *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, (Paris: FATF, 2014).

[69]FATF, *Guidance for a Risk-Based Approach… Op. Cit.*,par. 26 – 27

[70]Summarized from The Financial Action Task Force (FATF), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations 2012-2023, (Paris: FATF, 2023), pp. 16-17, 78-85.

a. *Recommendation No. 15 and Interpretative Notes*

Recommendation No. 15

- Countries should consider digital currencies as "property," "proceeds," "funds," "other funds or assets," or "related value." Therefore, countries must implement relevant measures based on FATF recommendations related to the prevention and prosecution of money laundering and terrorist financing crimes against digital currencies and VASPs;

- Countries must identify, assess, and understand the risks of money laundering, terrorist financing, and proliferation financing arising from digital currency activities and VASP service operations. Based on that assessment, countries should adopt a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the identified risks;

- Countries must ensure that virtual asset service providers (VASPs) are regulated for anti-money laundering and counter-terrorism financing purposes and are subject to an effective system to monitor and ensure compliance of virtual asset service providers with the relevant measures required in the FATF recommendations;

- The state must ensure that VASPs, whether individuals or legal entities, have a license or are registered, at least in the jurisdiction where they are established. The state must take action to identify individuals or legal entities conducting VASP activities without the necessary permits or registrations and impose appropriate sanctions;

- Countries must require VASPs to identify, assess, and take effective actions to mitigate the risks of money laundering, terrorist financing, and proliferation financing. VASP must be subject to an effective system to monitor and ensure compliance with national policies related to the prevention of money laundering and/or terrorist financing;

- Countries must ensure that there is a set of effective, proportional, and deterrent sanctions, whether criminal, civil, or administrative, available to address VASPs that fail to comply with anti-money laundering and/or counter-terrorism financing policies. Sanctions should be imposed not-

not only on VASPs but also on the individuals operating those VASPs;

- VASP must be supervised or monitored by competent authorities, who conduct risk-based supervision or monitoring and have adequate authority to oversee and ensure VASP's compliance with requirements to combat money laundering and terrorist financing. The mentioned authority includes conducting inspections, compelling VASPs to provide certain information, and imposing sanctions, as well as the authority to revoke, restrict, or suspend VASP licenses or registrations;

- The state must regulate in national law the obligation of VASP to conduct Customer Due Diligence (CDD) for every digital currency transaction amounting to USD/EUR 1,000. According to FATF Recommendation No. 10, the CDD is carried out in the following ways:

    - Identifying and verifying customer identity using reliable and independent sources of documents, data, or information;

    - Identifying the beneficial owner and taking reasonable steps to verify the identity of the beneficial owner, so that the VASP knows who the beneficial owner is. In the case where the beneficial owner is a legal entity, the VASP needs to understand the ownership and control structure of that entity;

    - Understanding and, if necessary, obtaining information about the purpose and nature of business relationships and transactions conducted;

    - Conducting ongoing due diligence on business relationships and monitoring transactions carried out during those relationships to ensure that the transactions are consistent with the VASP's knowledge of the customer, their business, and risk profile, including the source of funds.

- Countries must ensure that, in every digital currency transaction, both the originating and destination VASPs obtain and retain the necessary and accurate information about the profiles of the sender and beneficiary so that they can provide this information to the authorities upon request;

- Countries must provide international cooperation as quickly, constructively, and effectively as possible regarding money laundering, predicate offenses, and terrorism financing related to digital currencies. Specifically, VASP supervisors must exchange information quickly and constructively with their foreign partners, regardless of the nature or status of the supervisors and differences in nomenclature or VASP status;

- The provisions in Recommendation No. 16, such as monitoring the availability of information, implementing freezing actions, and prohibiting transactions against individuals or legal entities, also apply to digital currencies.

b. Recommendation No. 16 and Interpretative Notes

Recommendation No. 16

- This recommendation is also known as the "Travel Rule," including for digital currency transactions;

- Countries must ensure that financial institutions include the necessary and accurate information regarding the initiator of the transaction, the beneficiary, and the wire transfer transaction and related messages, and ensure that this information remains in the wire transfer or related messages throughout the payment chain;

- Countries must ensure that financial institutions monitor wire transfer transactions to detect transactions that lack information regarding the sender and/or recipient and take appropriate actions, such as freezing and prohibiting transactions by or with certain entities;

- Travel Rule is a key step in the anti-money laundering/terrorist financing regime that enables VASPs and financial institutions to prevent terrorist actors, money launderers, and other criminals by accessing wire transfers to move their funds, including digital currencies, and detecting if such-

misuse occurs. Specifically, the rules in the Travel Rule are intended to ensure that basic information about the sender and recipient in digital currency transactions is available for:

- Law enforcement authorities in order to detect, investigate, and prosecute criminals, as well as trace their assets;
- Financial intelligence unit to analyze suspicious or unusual activities;
- VASP and financial institutions that send, act as intermediaries, and receive transactions to identify and report suspicious transactions, as well as freeze funds and prevent transactions by or with certain entities.[71]

In addition to issuing the above recommendations, FATF also released specific guidelines that facilitate parties involved in digital currency transactions in preventing crimes involving digital currency. This guide contains certain red flag indicators to categorize a digital currency transaction as a suspected money laundering or terrorist financing transaction.[72] In fact, the FATF then issued guidelines regarding the actions that each of the aforementioned parties need to take, namely those in the public sector (such as financial transaction supervisors, law enforcement, etc.), the financial sector, and the non-financial sector[73], and VASP[74], in separate documents according to the roles of the parties involved.

---

[71]See also The Financial Action Task Force (FATF), *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, (Paris: FATF, 2023), p. 16.

[72]See The Financial Action Task Force (FATF), *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, (Paris: FATF, 2020).

[73]See The Financial Action Task Force (FATF), *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing: Public Sector*, (Paris: FATF, 2020).

[74]See The Financial Action Task Force (FATF), *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing: Financial and Non-financial Sectors*, (Paris: FATF, 2020).

2 Enforcement

In principle, enforcement related to digital currency does not need to wait for the occurrence of a crime. As mentioned earlier, FATF Recommendations No. 15 and 16 have enabled VASPs to freeze transactions if they are deemed suspicious based on red flag indicators or if they violate the Travel Rule.[75] Similar provisions have been adopted by the European Union for transactions that breach digital currency market regulations,[76] and by the United States for digital currency transactions of at least US$500,000, a process known as "administrative forfeiture."[77]

However, the provisions and mechanisms for enforcing digital currency regulations related to crimes still need to be established, given the potential for a digital currency transaction involved in a crime to not meet red flag indicators, rendering it non-suspicious or still compliant with the Travel Rule. In this context, a mechanism is necessary to secure or take control of the digital currency involved in such crimes so that it can later be confiscated as proceeds of crime or used to compensate victims affected by the crime. Conceptually, this mechanism involves the seizure, freezing, or confiscation of digital currency suspected of being connected to a crime, aiming to sever the owner's access to the currency to prevent its transfer, movement, sale, or other actions that could obscure or disguise ownership of the digital currency. Accordingly, this section will focus on enforcement actions such as seizure, freezing, or confiscation of digital currency suspected of being linked to criminal activities.

Essentially, the FATF has regulated the mechanisms for the seizure, freezing, and confiscation of digital currency in its 2019 Guidance on Financial Investigations Involving Virtual Assets. However, since this guidance is confidential and accessible only to FATF member states,[78] the provisions regarding the seizure, freezing, and confiscation of digital currency as stipulated by FATF cannot be elaborated upon-

---

[75]See also FATF, *Targeted Update on Implementation of the FATF Standard…, Op. Cit.*, p. 21.
[76]The European Parliament and the Council of the European Union, *markets in crypto-assets…, Op. Cit.*, Art. 94 par. 1.
[77]U.S. Department of Justice: Criminal Division, *Asset Forfeiture Policy Manual 2023*, (Washington: U.S. Department of Justice, 2023), p. 5.2.
[78]Nadine Schwarz, Ke Chen, dan Maksym Markevych, *Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations,* (Washington: International Monetary Fund, 2021), p. 15.

in this document. Nevertheless, FATF member states in the Latin American region, organized under the body known as GAFILAT, subsequently issued guidelines in 2021 for the investigation, identification, seizure, and confiscation of digital currency, which also heavily refer to the confidential FATF document. Some provisions regarding the seizure and confiscation of digital currency according to the GAFILAT guidelines are as follows:[79]

1. There are several general principles applicable to the seizure/freezing of digital currency, such as:

- The seizure or freezing of digital currency is similar to the seizure of other assets, as it must be carried out based on court authorization or order. Therefore, any party intending to seize/freeze digital currency must first seek authorization or obtain a court order before proceeding with the seizure/freezing. However, the party receiving the order and the mechanism for executing the seizure/freezing depend significantly on factors related to the digital currency in question, which must be determined prior to the seizure/freezing;

- Due to the higher level of technical complexity compared to the seizure of ordinary assets and the speed required to ensure successful seizure, the seizure or freezing of digital currency should ideally be conducted by trained and skilled personnel. Therefore, those carrying out such actions must be familiar with the various types of digital currency wallets and their security mechanisms;

- All seized digital currencies must be transferred to a wallet owned or managed by the state/government. This is crucial to prevent offenders or other parties from accessing or transferring the digital currency before the legal process is completed. Therefore, it is essential for law enforcement to identify the type of digital currency to be seized, and the state must have a dedicated wallet for each type of digital currency, as digital currencies can only be transferred to addresses compatible with their respective blockchains. For example, Bitcoin can only be sent to a Bitcoin address, Monero to a Monero address, and so on;

---

[79]Summarized from GAFILAT, *Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets*, (Buenos Aires: GAFILAT, 2021), p. 94 – 110. Lihat juga bagian "Annex I: Guidelines for Investigation, Identification, Seizure, and Confiscation of Virtual Assets", p. 118 – 142.

2. **In general, the seizure/freezing of digital currency is carried out in three (3) stages, namely: (i) planning the seizure; (ii) executing the seizure; and (iii) managing the assets post-seizure.**

3. **During the seizure planning stage, several steps that need to be taken include:**

- Identifying the type of digital currency to be seized/frozen, along with its transaction system and storage method. The first step is to determine whether the digital currency is transacted in a centralized manner by a central administrative authority, such as a company or entity that develops and operates the currency, or whether it is decentralized;

- If the digital currency transactions are conducted in a centralized manner, law enforcement can promptly request the court to issue authorization or an order for freezing or seizing the digital currency from the central authority;

- If digital currency transactions are conducted in a decentralized manner, law enforcement must identify whether the digital currency to be seized is stored in a custodial wallet,[80] where the private key required for transacting the digital currency is held and managed by a VASP. The follow-up actions based on this identification are:

  - If the digital currency and private key are stored by a VASP, law enforcement can immediately request the court to issue an order to freeze the digital currency, directing the VASP to transfer it to an address or wallet controlled by the state; or

  - If the digital currency and private key are not stored in a wallet managed by a VASP (non-custodial wallet),[81] the storage and management of the digital), the storage and management of the digital currency are directly-

---

[80] *A custodial wallet is a digital currency service where digital currency and/or user access tools (such as private keys) are held by the service provider on behalf of the user. Users interact with the service provider, rather than the blockchain, to manage their digital currency. Custodial wallets are also referred to as "hosted wallets." See* International Organization of Securities Commissions (IOSCO), *Policy Recommendations for Crypto and Digital Asset Markets: Final Report*, (Madrid, IOSCO, 2023), p. 45. See also International Organization of Securities Commissions (IOSCO), Issues, *Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms: Final Report*, (Madrid: IOSCO, 2020), p. 12 – 13.

[81] A non-custodial wallet is software or hardware that stores cryptographic keys for users, allowing digital currency to be accessed solely by the user and enabling them to interact directly with the blockchain and blockchain-based financial applications. Non-custodial wallets are also referred to as "unhosted wallets." See Ibid.

controlled by the offender. Therefore, the seizure must involve obtaining information about the private key or seed words that grant law enforcement access to the digital currency or wallet, enabling them to transfer the digital currency to a state-controlled wallet. In such cases, a request for court authorization to seize the digital currency must consider the following:

* The types of wallets controlled by the offender may include: (i) virtual wallets in the form of software stored on a desktop computer as an application or on a mobile phone, such as Mycelium, Greenbits, Breadwallet, and Airbitz; or (ii) hardware wallets that store private keys on portable devices, such as a pen drive or printed on paper;

* Therefore, law enforcement must request court authorization to seize all data storage devices found during searches, such as computers, mobile phones, portable hard drives, CDs, DVDs, memory sticks, flash drives, or other items that may contain information related to wallets, private keys, or seed words that can grant law enforcement access to the digital currency;

* Law enforcement should consider requesting court authorization to immediately seize digital currency if the device storing digital currency information is unlocked and active. This is because the ideal opportunity to access the digital currency arises when the wallet containing the private key is open, or when the password to unlock it or the "seed words" to access the wallet are discovered during the search;

* Law enforcement must also consider the need to immediately neutralize any possibility that the digital currency owner might destroy, alter, or hide information useful for accessing the digital currency wallet (e.g., handwritten passwords or PINs, hardware wallets, etc.), transfer the digital currency, or instruct others to do so before law enforcement successfully gains access to the wallet;

* Once law enforcement has obtained court authorization, they must promptly prepare a state-controlled wallet to receive the transfer of the digital currency to be seized, in accordance with the specific type of digital currency;

4. **During the execution stage of the seizure, several steps that need to be taken include:**

- Seizing the digital currency in accordance with its specific type or the type of wallet storing the digital currency (as detailed for each type of digital currency and wallet in the GAFILAT guidelines) and transferring the seized digital currency to a state-controlled wallet;

- Law enforcement must consider isolating the digital currency owner and all others present during the seizure process to prevent them from connecting to the Internet or contacting the outside world until the seizure is complete;

- If law enforcement discovers a device containing a wallet but the wallet is locked and the required password is not found, the device containing the wallet must be seized following procedures for handling electronic evidence. Subsequently, relevant investigative actions must be conducted promptly to obtain the password and seize the digital currency;

- If access to the wallet cannot be obtained or the wallet is found to be empty after being opened, law enforcement may identify the value of the digital currency to be seized through the blockchain and seize other assets of equivalent value to the digital currency;

- If the wallet is found to be unlocked, the seizure can be immediately carried out based on court authorization, and the seized digital currency can be transferred to a state-controlled wallet;

5. **In the post-seizure stage, several steps that need to be taken include:**

- In general terms, there are two (2) alternatives that can be undertaken regarding seized digital currency, namely:

  - **Maintaining the digital currency in its original form at the time of seizure until a verdict is rendered.**The advantage of this alternative is that the digital currency is sold only after a final judgment, allowing for its immediate return to the owner if the defendant is acquitted. However, the drawback lies in the inherent risks associated with securing the digital currency and the additional costs related to its maintenance;

  - **Maintaining the digital currency in its original form at the time of seizure until a judgment is rendered.** The advantage of this alternative is that the digital currency is sold only after a final judgment, allowing-

for its immediate return to the owner if the defendant is acquitted. However, the drawback lies in the inherent risks associated with securing the digital currency and the additional costs related to its maintenance;

- Another alternative is to establish, through regulations or internal policies, a fixed timeframe for converting seized digital currency into fiat currency (e.g., three days). This ensures that the decision to convert is not based on subjective economic considerations but rather on written rules established by the state;

- If it is decided to retain the digital currency in its original form, law enforcement must undertake the following actions:

  - Storing the digital currency in a cold wallet, such as a hardware wallet, a virtual wallet on a device not connected to the internet, or a paper wallet;

  - Storing passwords, private keys, seed words, PINs, and digital currency addresses in text files within dedicated folders for each seized digital currency on external storage devices, such as portable hard drives, which are then encrypted. These devices must remain offline in a secure location until needed by law enforcement;

  - Appointing specific officials to safeguard devices containing information such as passwords, private keys, seed words, PINs, and digital currency addresses, while restricting access to these devices;

  - If law enforcement lacks a reliable cybersecurity infrastructure for storing digital currency, they may appoint a trusted VASP to manage the digital currency;

- If it is decided to convert the digital currency into fiat currency, law enforcement must sell the digital currency, either directly or through a public auction, always striving to maximize the value of the sale. The conversion can also be carried out through an agreement with a VASP specializing in digital currency exchange to convert the digital currency into fiat currency;

- Some practices in certain countries regarding actions taken on seized digital currency are as follows:

  - In the Netherlands, decisions regarding actions on seized digital currency are made based on the written opinion of the digital currency owner, indicating whether they prefer the digital currency to be retained in its-

original form or converted into fiat currency. This approach ensures that if the digital currency must be returned later, the state is absolved of liability for any loss of value due to fluctuations in the digital currency's price;

- In the United States, digital currency is decided not to be converted into fiat currency but instead retained in its original form, with necessary security measures implemented to ensure its effective storage.

In general, the aforementioned provisions are similarly regulated in standards or guidelines related to the seizure, freezing, and confiscation of digital currency issued by other entities. These include guidelines published by StAR (the Stolen Asset Recovery Initiative), a collaboration between the World Bank Group and the United Nations Office on Drugs and Crime (UNODC),[82] and the European Union through the Cybercrime Programme Office of the Council of Europe (C-PROC).[83] Similar provisions can also be found in domestic laws and practices in several countries, such as the United Kingdom, which conducts the seizure, freezing, and confiscation of digital currency assets under the Proceeds of Crime Act 2002 (POCA),[84] the United States, which refers to general seizure rules under Rule 41 of the Federal Rules of Criminal Procedure and implements them technically in accordance with the Asset Forfeiture Policy Manual 2023 published by the U.S. Department of Justice,[85] and Malaysia, which technically carries out these actions based on guidelines issued by the National Anti-Financial Crime Center (NFCC) and CyberSecurity Malaysia (CSM).[86]

---

[82]Lisa Bostwick, dkk, *Managing Seized and Confiscated Assets: A Guide for Practitioners,* (Washington: World Bank, 2023), p. 174 – 175.

[83]The European Parliament and the Council of the European Union, *markets in crypto-assets…, Op. Cit.*, Art. 94 par. 3. For technical rules on the seizure, freezing, and confiscation of digital currency, see Cybercrime Programme Office of the Council of Europe (C-PROC), Guide On Seizing Cryptocurrencies, (Bucharest: C-PROC, 2021), ppl. 19 – 118.

[84]See United Kingdom, *Proceeds of Crime Act 2002* (POCA), Sections 47C(5A)–(5F), 47M(2A) and (2B), 47R(6), 67ZA, 67ZB, 67AA, 127C(5A)–(5F), 127M(2A) and (2B), 127Q(6), 131ZB, 131ZC, 131AA, 195C(5A)–(5F), 195M(2A) and (2B), 195R(6), 215ZA, 215ZB, 215AA, and Chapters 3C–3F. See also Skadden, "*Cryptoasset Seizures and Forfeitures…, Loc. Cit.*

[85]U.S. Department of Justice: Criminal Division, *Asset Forfeiture Policy Manual 2023…, Op. Cit.*, p. 2.10 – 2.12. . See also the internal technical regulations of local law enforcement in several U.S. states, such as Indiana (Indiana State Police, "Standard Operating Procedure: Seizure of Cryptocurrency and Virtual Currencies", https://www.in.gov/isp/files/Seizure-of-Cryptocurrency.pdf , Accessed on Friday, February 16, 2024) and Orlando (Orlando Police Department Policy and Procedure, "Policy 1411.0, Seizure of Cryptocurrency", https://www.orlando.gov/files/sharedassets/public/v/1/documents/opd/policies-and-procedures/investigative-procedures/1411.0-seizure-of-cryptocurrency.pdf, accessed on Friday, February 16, 2024).

[86]*National Anti-Financial Crime Center (NFCC) and CyberSecurity Malaysia (CSM), Policy and Procedure for Seizing Cryptocurrencies,* (Malaysia: NFCC dan CSM, 2023).

In general, the rules for preventing and combating money laundering and the financing of terrorism, including those involving digital currency, must be properly implemented by the entities required to do so. In this regard, strong cooperation and roles from institutions under the state, particularly those involved in anti-money laundering, are essential as competent authorities in enforcing these regulations. The European Union exemplifies this inter-institutional cooperation, which must involve numerous stakeholders, such as Financial Intelligence Units (FIUs), law enforcement agencies with investigative and prosecutorial functions related to money laundering, predicate crimes, and terrorist financing, authorities responsible for tracing, seizing, and freezing criminal assets, entities authorized to receive reports on cross-border currency transactions (including digital currencies), and authorities tasked with overseeing or monitoring compliance by certain entities with anti-money laundering regulations.[87]

In practice, the United States is one of the countries that has implemented inter-agency cooperation between government and law enforcement agencies in preventing and combating crimes involving digital currency. This was highlighted by U.S. Attorney General Merrick B. Garland as the rationale for establishing the Digital Asset Coordinator (DAC) Network on September 16, 2022, where cooperation across departments and agencies throughout the government is necessary to prevent and stop the exploitation of digital currencies to facilitate crime, as the role of digital currencies in the global financial system continues to grow. Assistant Attorney General Kenneth A. Polite Jr. further noted that the development of digital currencies has created a new landscape for exploiting this innovation by criminals, and the DAC was established to ensure that the U.S. Department of Justice and its prosecutors are in the best position to combat crimes involving digital currencies.[88]

Essentially, the DAC Network is not the first inter-agency cooperation forum or initiative in the prevention and prosecution of crimes involving digital currency in-

---

[87]The European Parliament and the Council of the European Union, *Amending Directive (EU) 2015/849…*, *Op. Cit.*, par. 44.
[88]U.S. Department of Justice, *Justice Department Announces Report on Digital Assets and Launches Nationwide Network*, Rilis Pers, Jum'at, 16 September 2022. Accessed at https://www.justice.gov/opa/pr/justice-department-announces-report-digital-assets-and-launches-nationwide-network. The DAC is led by the National Cryptocurrency Enforcement Team (NCET), a unit under the U.S. Department of Justice, with a network comprising more than 150 federal prosecutors appointed by U.S. Attorneys' Offices and all litigation components within the department. It will serve as the department's primary forum for prosecutors to obtain and disseminate specialized training, technical expertise, and guidance on the investigation and prosecution of crimes involving digital currency.

the United States. Several other units or initiatives were established prior to the formation of the DAC Network, including:[89]

2018

The Money Laundering and Asset Recovery Section (MLARS) under the U.S. Department of Justice's Criminal Division launched "the Digital Currency Initiative," which focuses on providing support and guidance to investigators, prosecutors, and other government agencies on the prosecution and seizure of digital currency;

2020

The Cyber-Digital Task Force under the Attorney General launched "the Cryptocurrency Enforcement Framework," which outlines the legal tools available for prosecuting illegal use of digital currency, profiles the roles and responsibilities of each department and government agency in the field of digital assets/currencies, and outlines strategies to address emerging threats to the security and effective operation of digital currency markets;

2021

The U.S. Department of Justice announced the formation of the National Cryptocurrency Enforcement Team (NCET), which includes federal prosecutors, investigators, and other supporting staff such as experts from MLARS, U.S. Attorneys' Offices, the FBI, and financial regulators. NCET's priority tasks include developing strategies related to digital currency technology, identifying areas for enhanced investigative and prosecutorial focus, addressing issues arising from the application of existing regulations to digital currency use, and leading the Department's efforts to coordinate with domestic and international law enforcement partners, regulatory bodies, and the private sector to combat crimes involving digital currency;

2022

The FBI established the Virtual Asset Exploitation Unit (VAXU), a specialized team dedicated to investigating crimes involving digital currency. VAXU was created to bring together digital currency experts within a single unit to provide the necessary tools and technology, blockchain analysis, digital currency seizure training, and other digital currency-related training for FBI personnel. Working closely with NCET, this unit also includes prosecutors with expertise in money laundering, computer crimes, asset seizure, and policy/regulatory development to pursue individuals who misuse digital currency for criminal activities.[90]

---

[89]U.S. Department of Justice, T*he Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067: The Role of Law Enforcement In Detecting, Investigating, and Prosecuting Criminal Activity Related To Digital Assets*, (Washington: U.S. Department of Justice, 2022), p. 14 – 16.

[90]As stated by U.S. Deputy Attorney General Lisa O. Monaco in her remarks at T*he Annual Munich Cyber Security Conference*, Washington D.C., on Thursday, February 17, 2022. The full text is available at: https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security

B. Regulations and Practices Related to the Prevention and Prosecution of Crimes Involving Digital Currency in Indonesia

Currently, digital currency transactions are one of the financial activity options in Indonesia. According to the Commodity Futures Trading Supervisory Agency/Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti), digital currency transactions were recorded at Rp859.4 trillion in 2021, Rp306.4 trillion in 2022, and Rp149.25 trillion in 2023, with expectations of growth in 2024. Additionally, as of now, 501 officially registered digital currencies and 33 regulated Crypto Asset Physical Traders (digital currency traders) are listed under Bappebti.[91]

The recognition of digital currency in Indonesia was first regulated under Minister of Trade Regulation No. 99 of 2018 on General Policies for the Implementation of Futures Trading of Crypto Assets. This regulation was issued in response to the widespread use of crypto assets/digital currencies in society and aimed to protect the public while providing legal certainty for businesses in the Futures Trading sector.[92] Under this regulation, crypto assets were designated as commodities that can be traded on the Futures Exchange, with their guidance, supervision, and development delegated to the Head of Bappebti.[93] To implement this regulation, Bappebti issued two (2) technical rules, namely:

1. Bappebti Regulation No. 5 of 2019 in conjunction with Bappebti Regulation No. 3 of 2020, which essentially governs the technical rules for trading crypto assets on the futures exchange.[94] This regulation was later updated by Bappebti Regulation No. 8 of 2021 in conjunction with Bappebti Regulation No. 13 of 2022;[95]

2. Bappebti Regulation No. 7 of 2020, which initially listed 229 digital currencies that were registered and allowed to be traded in Indonesia.[96] Bappebti later updated this regulation by increasing the number of registered and tradable digital currencies in Indonesia to 510 through Bappebti Regulation No. 11 of 2022 in conjunction with Bappebti Regulation No. 4 of 2023.[97]

---

[91]Kementerian Perdagangan RI, "Bappebti Targetkan Transaksi Kripto Rp800 Triliun pada 2024", https://www.kemendag.go.id/berita/pojok-media/bappebti-targetkan-transaksi-kripto-rp800-triliun-pada-2024 , accessed on Friday, March 1, 2024.
[92]Minister of Trade Regulation of the Republic of Indonesia No. 99 of 2018 on General Policies for the Implementation of Futures Trading of Crypto Assets (Crypto Asset), section "Considering," letters b and c.
[93]Ibid., Article 1 and 2.
[94]See Bappebti Regulation No. 5 of 2019 in conjunction with Bappebti Regulation No. 3 of 2020 on Technical Provisions for the Implementation of the Physical Market for Crypto Assets on the Futures Exchange.
[95]See Bappebti Regulation No. 8 of 2021 in conjunction with Bappebti Regulation No. 13 of 2022 on Guidelines for the Implementation of the Physical Market Trading of Crypto Assets on the Futures Exchange.
[96]See Bappebti Regulation No. 7 of 2020 on the Determination of the List of Crypto Assets Tradable in the Physical Market of Crypto Assets.
[97]Bappebti Regulation No. 11 of 2022 in conjunction with Bappebti Regulation No. 4 of 2023 on the Determination of the List of Crypto Assets Tradable in the Physical Market of Crypto Assets.

In general, the above regulations have accommodated provisions for preventing the involvement of digital currencies in crimes, as outlined in FATF Recommendations and Interpretive Notes for Recommendations No. 15 and 16. For instance, they include requirements and mechanisms for digital/crypto currencies to be traded in Indonesia,[98] conditions and obligations for Futures Exchanges,[99] Crypto Asset Physical Traders,[100] and Crypto Asset Storage Managers to operate in Indonesia,[101] the obligation of Crypto Asset Physical Traders to implement Know Your Customer (KYC), Customer Due Diligence (CDD),[102] and Know Your Transaction (KYT) principles,[103] as well as the right of Crypto Asset Physical Traders to reject potential Crypto Asset Customers based on KYC and CDD results,[104] the requirements and mechanisms for crypto asset trading,[105] covering account opening, fund and crypto asset placement, crypto transactions, and crypto asset withdrawals, as well as the institutions supervising crypto trading,[106] among others. Furthermore, the above regulations also stipulate sanctions for parties violating crypto asset trading rules.[107] Notably, these regulations specifically address the "Implementation of Travel Rule Principles," which align with FATF Recommendation No. 16.[108]

Along with the growth of digital currency transactions, several crimes in Indonesia have also involved digital currencies. This has been acknowledged by the PPATK, which stated that one modus operandi for money flows in money laundering cases, particularly those involving fraudulent or illegal investments, is storing funds in the form of digital/crypto currencies.[109] In fact, there have been several cases involving digital currencies, such as the PT Asabri (Persero) corruption case, which allegedly included money laundering activities through Bitcoin,[110] the case of Indra Kesuma, also known as Indra Kenz, who committed fraud-

---

[98]Bappebti Regulation No. 8 of 2021 in conjunction with Bappebti Regulation No. 13 of 2022..., Op. Cit., Article 3.
[99]*Ibid.*, Articles 5 – 8.
[100]*Ibid.*,Articles 13–16 and 40–42. See also Bappebti Regulation No. 11 of 2022 in conjunction with Bappebti Regulation No. 4 of 2023..., Op. Cit., Articles 1 and 8.
[101]*Ibid.*, Articles 17 – 22.
[102]*Ibid.*, Articles 26 – 28 dan Articles 32 paragraphs (3) and (4).
[103]*Ibid.*, Articles 39.
[104]*Ibid.*, Articles 16 ayat (3) letter a.
[105]*Ibid.*, Articles 25 – 37.
[106]Initially, the supervision of digital/crypto currency trading fell under the authority of Bappebti. See Ibid., Article 1 point 1. However, over time, this supervisory authority shifted to the Financial Services Authority (OJK). See Law No. 21 of 2011 on the Financial Services Authority in conjunction with Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector, Article 6 paragraph (1) letter e.
[107]*Ibid.*, Articles 47–49. See also Bappebti Regulation No. 11 of 2022 in conjunction with Bappebti Regulation No. 4 of 2023..., Op. Cit., Article 9.
[108]Bappebti Regulation No. 8 of 2021 in conjunction with Bappebti Regulation No. 13 of 2022..., Ibid., Article 38.
[109]"Optimalisasi Pengembalian Aset & Keuangan Negara: PPATK Perkuat Analisis & Pemeriksaan Transaksi Keuangan", PPATK, April 15, 2022, https://www.ppatk.go.id/siaran_pers/read/1188/optimalisasi-pengembalian-aset-keuangan-negara-ppatk-perkuat-analisis-pemeriksaan-transaksi-keuangan.html.
[110]Novina Putri Bestari, "Saat Cuci Uang di Bitcoin Jadi Modus Baru Korupsi Asabri", CNBC Indonesia, April 21, 2021, https://www.cnbcindonesia.com/tech/20210420232119-37-239412/saat-cuci-uang-di-bitcoin-jadi-modus-baru-korupsi-asabri.

and had crypto assets worth Rp35 billion seized,[111] and the case of Donny Alven, who hacked crypto accounts from 2017 to 2024, resulting in the seizure of assets totaling Rp5.1 billion.[112]

However, law enforcement officers in Indonesia still face significant challenges in handling crypto assets or digital currencies linked to criminal activities. There are at least two primary factors contributing to these difficulties: the lack of comprehensive regulations concerning crypto assets, particularly regarding their seizure, and the limited experience and knowledge of law enforcement regarding crypto assets and their management.[113] In practice, these obstacles are evident in cases such as the failure of law enforcement to seize Bitcoin owned by Heru Hidayat and Benny Tjokrosaputro at a Crypto Asset Physical Trader named Indodax, which allegedly served as a repository for proceeds of corruption in the PT ASABRI case, as the Bitcoin account was empty when the seizure was attempted.[114] Additionally, there are potential barriers, such as the case experienced by prosecutors in Kempten, Germany, where they successfully seized a Bitcoin wallet containing 1,700 BTC worth over £50 million (approximately Rp841 billion) but were unable to access the wallet because the owner refused to provide the password.[115] For this reason, comprehensive regulations on the management, particularly the seizure, of digital currencies/crypto assets related to criminal activities are urgently needed in Indonesia.

To date, the provisions for handling digital currencies related to criminal activities have only been regulated as of 2023 by the Attorney General's Office through Attorney General Guidelines No. 7 of 2023 on the Handling of Crypto Assets as Evidence in Criminal Cases. These guidelines primarily regulate the following:

---

[111]Putranegara Batubara, "Aset Kripto Indra Kenz Rp35 Miliar Bakal Disita Bareskrim", *IDX Channel*, 22 April 2022, https://www.idxchannel.com/economics/aset-kripto-indra-kenz-rp35-miliar-bakal-disita-bareskrim.

[112]"Gagal Jadi Crazy Rich, Peretas Kripto Pekanbaru Ditangkap & Kekayaannya Disita", *Kumparan*, 12 January 2024, https://kumparan.com/kumparannews/gagal-jadi-crazy-rich-peretas-kripto-pekanbaru-ditangkap-and-kekayaannya-disita-21xBpj9LqAl/1.

[113]Jefferson Hakim, "Langkah Maju Kejaksaan dalam Penyitaan Aset Kripto", *Hukum Online*, 31 January 2024,https://www.hukumonline.com/berita/a/langkah-maju-kejaksaan-dalam-penyitaan-aset-kripto-lt65b9ac6bc31c8/?page=1.

[114]Angga Bratadharma, "Diduga Gagal Buktikan Aliran Dana Bitcoin di ASABRI, Kejagung Diminta Tak Beropini", *Medcom*, 23 June 2021, https://www.medcom.id/ekonomi/keuangan/akWxw0aK-diduga-gagal-buktikan-aliran-dana-bitcoin-di-asabri-kejagung-diminta-tak-beropini.

[115]Panca Saujana, "1700 BTC, Jaksa Jerman: Mana Password Dompet Bitcoin-nya?", *Blockchain Media*, 5 February 2021, https://blockchainmedia.id/1700-btc-jaksa-jerman-mana-password-dompet-bitcoin-nya/

1. A request for approval or authorization to seize digital currency/crypto assets must be submitted to the Chief of the District Court in accordance with the seizure provisions in the Indonesian Criminal Procedure Code (KUHAP). In cases where the crypto assets are located abroad, the request for approval or authorization must be submitted to the Chief of the Central Jakarta District Court;[116]

2. The blocking of accounts and wallets during the seizure of crypto assets is carried out by the Digital Evidence First Responder (DEFR) upon the orders of the prosecutor/investigator. DEFR refers to a competent or expert employee assigned to handle the initial management of crypto assets, with the responsibility of managing the crypto assets;[117]

3. The blocking of crypto assets is only conducted on centralized crypto assets through Crypto Asset Physical Traders. Decentralized crypto assets, however, cannot be subjected to blocking;[118]

4. Seized crypto assets can be secured by being transferred by the DEFR from the owner's wallet to a Controlled Cryptowallet, which is in the form of a hardware wallet and corresponds to the type of seized crypto asset. This transfer is conducted if the value of the crypto assets is considered significant and/or based on considerations related to the effectiveness of case handling;[119]

5. *he Controlled Cryptowallet and Controlled Address are created by officials responsible for managing evidence and confiscated goods at the request of the prosecutor, both before and after the seizure, and are tailored to the crypto assets to be seized. These officials are also authorized to secure, monitor, and manage the seized crypto assets, including the private key of the Controlled Cryptowallet and Controlled Address;*[120]

---

[116]Attorney General Guidelines No. 7 of 2023 on the Handling of Crypto Assets as Evidence in Criminal Cases, Chapter IV "Request for Court Approval and Authorization," pp. 9–10.
[117]Ibid., p. 4 and 7.
[118]Ibid., p. 7.
[119]Ibid., p. 6 – 8.
[120]Ibid., p. 6 and 11.

6. After the seizure, the handling of crypto assets prioritizes maintaining their original form without conversion into Indonesian Rupiah (cash). However, if the crypto assets are unregistered and/or the management costs without conversion are excessively high, the crypto assets may be converted into Indonesian Rupiah (cash), with or without the asset owner's consent;[121]

7. Crypto assets, whether converted or not, along with the Controlled Cryptowallet and Controlled Address, are stored in a designated room within the evidence storage area and are periodically monitored by officials responsible for managing seized assets, evidence, and confiscated goods;[122]

8. Any reduction in the value of crypto assets and/or costs incurred due to the transfer and/or conversion of crypto assets is deducted from the value of the seized crypto assets and will subsequently be stated in the indictment.[123]

Upon closer examination, Attorney General Guidelines No. 7 of 2023 have generally regulated provisions similar to international standards established by FATF, GAFILAT, the European Union, and other previously mentioned institutions. This can be observed from provisions that refer to general principles in the seizure of digital currency, such as conducting seizures based on court authorization, ensuring seizures are carried out by officers with specific knowledge and competence, and securing seized assets by transferring them to wallets controlled by the state. Additionally, the guidelines also emphasize the authority responsible for securing, supervising, and managing seized digital currencies, including private keys of Controlled Cryptowallets and Controlled Addresses. Furthermore, mechanisms for handling seized digital currencies, whether through conversion into Indonesian Rupiah or non-conversion, are also addressed, as well as provisions related to the depreciation of digital currency value.

[123]Ibid., 8.
[124]Ibid., p. 10.
[123]Ibid., p. 11.

IV.

OPPORTUNITIES AND CHALLENGES IN REGULATING DIGITAL CURRENCY IN RELATION TO LAW ENFORCEMENT IN INDONESIA

A. Opportunities and Challenges: Regulations in the Prevention Framework

As outlined in Section III, the trading of crypto assets as futures commodities in Indonesia is currently regulated and supervised by Bappebti. Based on the series of regulations issued by Bappebti, the various actors involved in crypto asset trading in Indonesia are as follows:

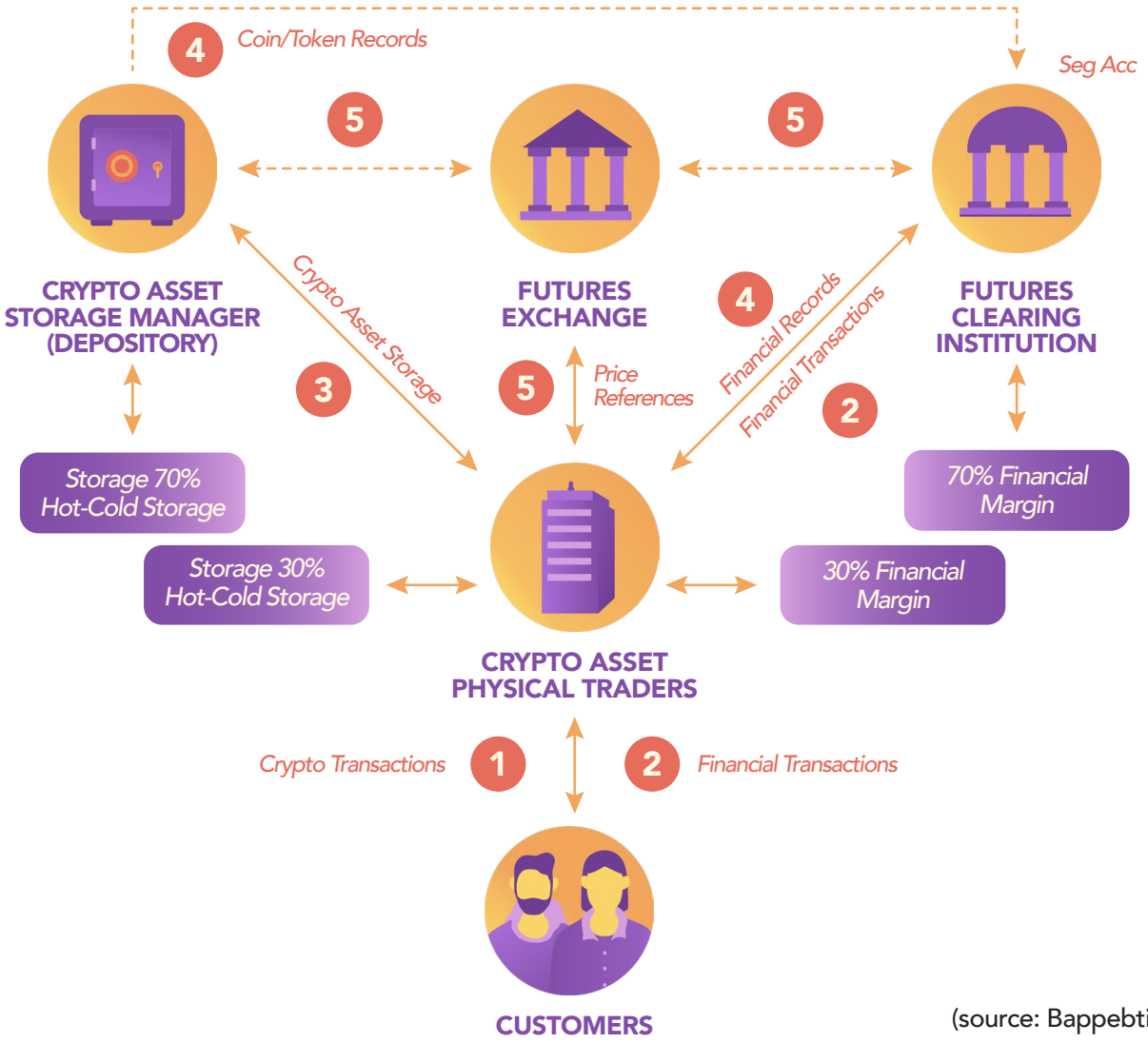
Table 5. Actors in Crypto Asset Trading in Indonesia

Actor	Definition	Description
Crypto Asset Futures Exchange	A business entity that organizes and provides systems and/or facilities for the buying and selling of commodities based on Futures Contracts, Sharia Derivative Contracts, and/or other Derivative Contracts.	The registered futures exchange is PT Bursa Komoditi Nusantara.[124]
Futures Clearing Institution	A business entity that organizes and provides systems and/or facilities for clearing and guaranteeing the settlement of Futures Trading transactions.	The registered futures clearing institutions are PT Kliring Berjangka Indonesia and PT Kliring Komoditi Indonesia.[125]
Prospective Crypto Asset Physical Traders (Exchangers)	Entities that have obtained a registration certificate from the Head of Bappebti to conduct transactions related to Crypto Assets, either on their own behalf and/or by facilitating Crypto Asset Customers, while the Crypto Asset Futures Exchange and Crypto Asset Futures Clearing Institution are not yet established.	As of the time this document was written, at least 35 companies are registered as prospective crypto asset physical traders.[126]
Crypto Asset Storage Manager (Depository)	An entity that has obtained approval from the Head of Bappebti to manage a storage facility for Crypto Assets, including their safekeeping, maintenance, supervision, and/or delivery.	The registered crypto asset storage managers are PT Tennet Depository Indonesia and PT Kustodian Koin Indonesia.[127]
Crypto Asset Customers	Parties who use the services of Crypto Asset Physical Traders to buy or sell Crypto Assets traded in the Physical Crypto Asset Market.	

[124]"Bursa Berjangka Penyelenggara Perdagangan Aset Kripto", diakses melalui: https://bappebti.go.id/bursa_kripto, March 31, 2024.
[125]"Kliring Berjangka Aset Kripto," diakses melalui: https://bappebti.go.id/kliring_kripto, March 31, 2024.
[126]"Calon Pedagang Fisik Aset Kripto", Laman Resmi Bappebti, diakses melalui https://bappebti.go.id/calon_pedagang_aset_kripto March 31, 2024.
[127]"Pengelola Tempat Penyimpanan Aset Kripto", diakses melalui https://bappebti.go.id/penyimpanan_kripto March 31, 2024.

The roles of each of the actors mentioned above can be further understood through the flow of crypto asset trading in Indonesia, as outlined below:

Diagram of the Crypto Asset Trading Flow in Indonesia



(source: Bappebti)

From this flow, the only actor that directly interacts with crypto asset customers is the Crypto Asset Physical Trader (exchanger). Therefore, the obligation to implement KYC, CDD, KYT, and Travel Rule principles generally applies solely to exchangers. Consequently, customers wishing to transact crypto assets in Indonesia must first verify their identity with the exchanger. Once identity verification is completed, customers can proceed with transactions by depositing funds, where 70% of the funds are held by the Clearing Institution and 30% by the exchanger.

The transacted crypto assets are then stored with the following allocation: at least 70% of the crypto assets are held by the depository, and a maximum of 30% are held by the exchanger. Specifically for exchangers, the storage of crypto assets is further divided as follows: at least 70% offline (cold wallet) and a maximum of 30% online (hot wallet).

In addition, exchangers are also required to submit financial records to the Clearing Institution, which include records of crypto asset ownership. Based on these financial records, the Clearing Institution performs a verification function to ensure the financial amounts align with the crypto assets stored by the Crypto Asset Storage Manager (Depository). Using transaction data reported by the exchanger, Clearing Institution, and Depository, the Futures Exchange then carries out its market supervision function and issues price references used by the exchanger.

Bappebti further explains that for "crypto assets that have been transacted, (public and private keys) will be stored by the Crypto Asset Commodity Trader in the depository, whether in the form of Hot Wallets or Cold Wallets."[128] Linking this to the discussion in Section II regarding types of wallets, Bappebti's explanation can be interpreted as the use of custodial wallets, where users' private keys are centrally stored by a third party, in this case, the exchanger and/or depository in Indonesia.

This is closely related to efforts to enforce action against crypto assets in the event of a criminal offense, as custodial wallets enable law enforcement authorities (APH) to directly coordinate with exchangers and/or depositories in Indonesia to gain access to the crypto assets. This differs significantly from the use of non-custodial wallets, where private keys are entirely managed by the crypto asset customers. In such cases, enforcement of crypto assets heavily depends on the willingness of the crypto asset customers to cooperate with law enforcement by handing over the private key or on the ability of law enforcement to locate the private key themselves. Therefore, it can be concluded that Bappebti's regulatory framework mandating the use of custodial wallets in Indonesia presents an opportunity to mitigate potential obstacles in the process of enforcing actions against crypto assets in the country.

Freezing Crypto Assets Based on Red Flag Indicators

Nevertheless, from the Asabri case, we can identify another obstacle that arises in the process of enforcing actions against crypto assets: the condition where the suspect transfers crypto assets during the investigation process. This highlights the crucial role of exchangers in identifying suspicious transactions before a criminal act occurs. As previously discussed in Section III, through Recommendations No. 15 and 16, FATF has-

---

[128]Perdagangan Aset Kripto" (Badan pengawas Perdagangan Berjangka Komoditi (Bappebti)), 2021, p. 12, accessed on https://bappebti.go.id/resources/docs/brosur_leaflet_2001_01_10_7zwvgs5w.pdf.

authorized VASPs to freeze transactions when suspicious activity is detected based on red flag indicators. Some of the red flag indicators identified by FATF are closely related to:[129]

#1 **Transaction size and frequency,** such as conducting repeated small transactions to avoid specific reporting obligations or executing transactions with multiple parties operating in other countries.

#2 **Irregular, unusual, or abnormal transaction patterns,** such as new users making large initial deposits inconsistent with their customer profile, engaging in transactions involving multiple virtual assets, or managing numerous accounts without a logical business explanation.

It is crucial to highlight whether these recommendations are integrated (or not) into the regulations concerning KYT, which is inherently tied to exchangers as the sole actors directly interacting with crypto asset customers in Indonesia. Bappebti Regulation No. 8 of 2021 in conjunction with Bappebti Regulation No. 13 of 2022, particularly Article 39, stipulates that as part of the KYT obligation, exchangers must monitor and review the crypto asset transactions they facilitate, enabling the identification of suspicious transactions. This monitoring and review are conducted using Regtech through blockchain analytic tools, either paid or open-source. Furthermore, Article 16 mandates that exchangers report such suspicious transactions to the Head of PPATK.

At least two challenges can be highlighted regarding the use of Regtech in identifying suspicious transactions. First, whether the indicators employed by blockchain analytic tools align with the red flag indicators recommended by FATF. Second, the extent of Bappebti's oversight of exchanger compliance with KYT obligations. Ensuring the suitability of red flag indicators used by exchangers to identify suspicious transactions is critical, as inadequate indicators increase the likelihood of suspicious transactions being undetected by blockchain analytic tools. Therefore, adopting FATF-recommended red flag indicators for crypto asset transactions into KYT obligations for exchangers in Indonesia is essential. This effort must be carried out in parallel with strengthening Bappebti's supervisory functions to ensure oversight extends beyond merely verifying the use of blockchain analytic tools to evaluating whether the indicators employed in those tools meet applicable international standards, particularly those recommended by FATF.

---

[129] "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing: Virtual Asset Service Providers" (FATF, September 2020), p. 3, accessed on www.fatf-gafi.org/publications/atfrecommendations/documents/VirtualAssets-Red-Flag-Indicators.html

B. Opportunities and Challenges: Regulations in the Enforcement Framework

In the previous chapter, it was outlined that Indonesia currently has only one regulation governing the enforcement of actions against digital currencies related to criminal activities, namely Attorney General Guidelines No. 7 of 2023. This regulation aligns with international standards established by FATF, GAFILAT, the European Union, and other institutions, adhering to general principles for the seizure of digital currencies and emphasizing the authority responsible for the security, supervision, and management of seized digital currencies. However, several notes should be taken into consideration regarding Attorney General Guidelines No. 7 of 2023, which could also pose challenges in enforcing laws against digital currencies involved in criminal activities, including:

1. Attorney General Guidelines No. 7 of 2023 is an internal regulation of the Attorney General's Office, and thus it only binds law enforcement officers under this institution. However, the seizure of digital currencies can occur during the investigation process, where the Attorney General's Office is only authorized to conduct investigations in specific cases, while general investigative functions are carried out by police investigators and Civil Servant Investigators (PPNS). As such, the provisions in Attorney General Guidelines No. 7 of 2023 may not be applied to every criminal offense involving digital currencies, especially those not investigated by the Attorney General's Office;

2. Attorney General Guidelines No. 7 of 2023 only regulate seizure procedures for centralized digital currencies and explicitly state that such actions cannot be taken for decentralized digital currencies. However, a distinctive characteristic of digital currencies often exploited for criminal purposes is their decentralized nature. Moreover, as previously discussed, international standards provide that the seizure of decentralized digital currencies is also possible through VASPs (or Crypto Asset Physical Traders or Crypto Asset Storage Managers in the Indonesian context) if the digital currencies and private keys are stored by VASPs (custodial wallets). Additionally, seizure can include all data storage devices that may contain information related to wallets, private keys, or seed words, in cases where the digital currencies and private keys are not stored in VASP wallets but are directly controlled by the digital currency owners (non-custodial wallets);

3. Attorney General Guidelines No. 7 of 2023 rely heavily on the involvement of DEFR (Digital Evidence First Responder) for the seizure of digital currencies and their transfer to a Controlled Cryptowallet, particularly for centralized digital currencies. However, as outlined in the previously discussed standards, the blocking or seizure of centralized digital currencies does not necessarily require DEFR assistance and can be executed directly by law enforcement through an order to the central authority managing the digital currency, based on a court warrant, to block/seize and transfer the offender's digital currency to a Controlled Cryptowallet. The role of DEFR is fundamentally more critical in the seizure of decentralized digital currencies held in non-custodial wallets, a scenario not addressed in these guidelines. Such cases involve handling electronic devices that may store information related to digital currencies, where DEFR expertise is essential for managing and securing the assets effectively.[130]

Based on these considerations, it can be concluded that the current regulations on the enforcement of digital currency actions related to criminal offenses differ from those on prevention. While the regulations on preventing the involvement of digital currencies in crimes are aligned with international standards, Indonesia still lacks sufficient rules for enforcing actions against digital currencies related to criminal offenses, particularly in the context of blocking or seizure. Therefore, Indonesia requires additional regulations on digital currencies, particularly regarding procedural mechanisms for the seizure/blocking of digital currencies, to establish a more comprehensive legal framework for handling digital currencies associated with criminal offenses. Some provisions that need to be addressed and regulated in this context include:

1. **Establishing regulations on the enforcement of actions against digital currencies related to criminal offenses, particularly blocking or seizure, within criminal procedural law at the legislative level**. This is necessary to create a standardized mechanism for enforcing actions against digital currencies linked to crimes, applicable to all types of offenses and all law enforcement agencies. Given the diversity of law enforcement institutions in Indonesia, including the police,-

[130]This is because the primary function of DEFR is to handle electronic devices to search for digital evidence stored within them. See ISO 27037: Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence, p. 2.

the Attorney General's Office, and Civil Servant Investigators (PPNS) in specific crimes such as environmental, forestry, and fisheries offenses, and more.[131] With such a provision in criminal procedural law, law enforcement agencies would not apply varying practices for handling digital currencies in different cases, thereby ensuring legal certainty in the procedural rules for addressing digital currencies involved in criminal offenses in Indonesia.

Furthermore, regulating the enforcement of digital currency actions at the legislative level is essential to ensure that such actions align with human rights principles. It is important to recognize that blocking or seizure inherently constitutes a violation of the right to privacy and ownership of property, as enshrined in human rights principles within the Indonesian Constitution,[132] the Human Rights Law,[133] and international human rights regulations.[134] In other words, blocking or seizure represents a limitation on the enjoyment of privacy and property rights imposed by the state. Therefore, the implementation of such actions must comply with permissible human rights limitations to prevent arbitrary conduct. Considering that one of the prerequisites for limiting human rights is that such limitations must be established in national legislation, **it is imperative that regulations on enforcing actions against digital currencies are codified within criminal procedural law at the legislative level**.

2. Several general provisions that need to be regulated with reference to the international standards previously outlined include, at a minimum, the following:

   a. Seizure or freezing of digital currencies must be carried out based on court authorization. In other words, any law enforcement officer wishing to seize/freezing digital currency must first seek authorization or obtain an order from the court before proceeding with the-

---

[131]Muhammad Tanziel Aziezi dan Arsil, *Asesmen Sistem Peradilan Pidana di Indonesia*, (Jakarta: Kemitraan Partnership, 2023), p. 76.
[132]The Constitution of the Republic of Indonesia 1945, Article 28G paragraph (1).
[133]Law No. 39 of 1999 on Human Rights, Article 29 paragraph (1).
[134]Universal Declaration of Human Rights (UDHR), Article 17 paragraph (2).
See also the International Covenant on Civil and Political Rights (ICCPR), General Assembly Resolution No. 2200A (XXI), December 16, 1966, Article 17 paragraph (1).

seizure/freezing. The court order for seizure/freezing must specify the identity of the party against whom the seizure/freezing is to be carried out;

b. All seized digital currencies must be transferred to a wallet that corresponds to the type of each digital currency owned or managed by the state/government to prevent the offender or other parties from accessing or transferring the digital currency before the legal process is completed;

c. All information related to the seizure/freezing actions, including the amount or number of seized digital currencies and the wallet where the seized digital currency is stored, must be included in the minutes of the seizure as referred to in Article 75 of the Indonesian Criminal Procedure Code (KUHAP);

3. Regulating that the seizure/freezing of digital currencies is carried out in three (3) stages, namely: (i) planning; (ii) execution; and (iii) post-seizure;

4. Regulating that law enforcement must undertake several actions during the planning stage, including:

a. Identifying the type of digital currency to be seized/frozen, along with its transaction system and storage method, in order to determine the party to be subject to seizure/freezing and the wallet needed to store the seized/frozen digital currency;

b. Identifying the type of digital currency to be seized/frozen, along with its transaction system and storage method, in order to determine the party to be subject to seizure/freezing and the wallet needed to store the seized/frozen digital currency:

- If the digital currency transaction is conducted in a centralized manner by a central administrative authority, law enforcement must request the court to issue an order to freeze or seize the digital currency from the central authority, which will then freeze and transfer the digital currency to an address or wallet controlled by the state;

- If the digital currency transaction is decentralized and the digital currency and private key are stored by a Crypto Asset Physical Trader or Crypto Asset Storage Manager (custodian wallet), law enforcement must request the court to issue an order to freeze the digital currency from the Crypto Asset Physical Trader or Storage Manager, which will then freeze and transfer the digital currency to an address or wallet controlled by the state;

- If the digital currency transaction is decentralized and the digital currency and private key are not stored in a wallet owned by a Crypto Asset Physical Trader or Crypto Asset Storage Manager (non-custodial wallet), then:

    - Law enforcement needs to request court authorization to seize all data storage devices found during the search, such as computers, mobile phones, portable hard drives, CDRs, DVDRs, memory sticks, flash drives, or other items that may store information related to wallets, private keys, or seed words that would grant law enforcement access to the digital currency, such as hardware wallets that store private keys on portable devices, like pen drives or printed on paper;

    - Law enforcement should consider requesting court authorization to immediately seize the digital currency and transfer it to a government-controlled wallet if the information storage device is found unlocked and active;

C Once law enforcement has obtained court authorization, they must promptly prepare a state-controlled wallet to receive the transfer of the digital currency to be seized, in accordance with the type of digital currency involved;

5. Regulating several actions that law enforcement must undertake during the execution stage, including:

   a. Seizing digital currency in accordance with its type or the wallet used to store the digital currency and transferring the seized digital currency to a state-controlled wallet;

   b. For the seizure of decentralized digital currencies stored using a non-custodial wallet method, the seizure must be carried out by personnel with the expertise and skills to handle the seizure of various types of digital wallets and their security mechanisms;

   c. Law enforcement may isolate the digital currency owner and all others present during the seizure process to prevent them from connecting to the Internet or making contact with the outside world until the seizure is completed;

   d. If the wallet is found unlocked, law enforcement is authorized to directly seize and transfer the seized digital currency to a state-controlled wallet in accordance with the court's authorization;

   e. If law enforcement finds a device storing a wallet, but the wallet is locked and the required password cannot be found, the device containing the wallet should be seized following procedures for handling electronic evidence. Law enforcement must then conduct relevant investigations promptly to obtain the password and seize the digital currency;

   f. If access to the wallet cannot be obtained, or if the wallet is found empty after being opened, law enforcement may identify the value of the digital currency to be seized through the blockchain and seize other assets of equivalent value;

6. Regulating that law enforcement is required to record all information related to the seizure/freezing actions, including the amount or number of seized digital currencies and the wallet where the seized digital currency is stored, in the minutes of the seizure as referred to in Article 75 of the Indonesian Criminal Procedure Code (KUHAP) after the seizure is conducted;

7 Determining the mechanism for managing digital currencies already stored in state-controlled or government-controlled wallets with the following alternatives, among others:

a **Retaining the digital currency in its original form at the time of the seizure until a verdict is rendered**. If this mechanism is chosen for asset management, the following provisions must be adhered to, including:

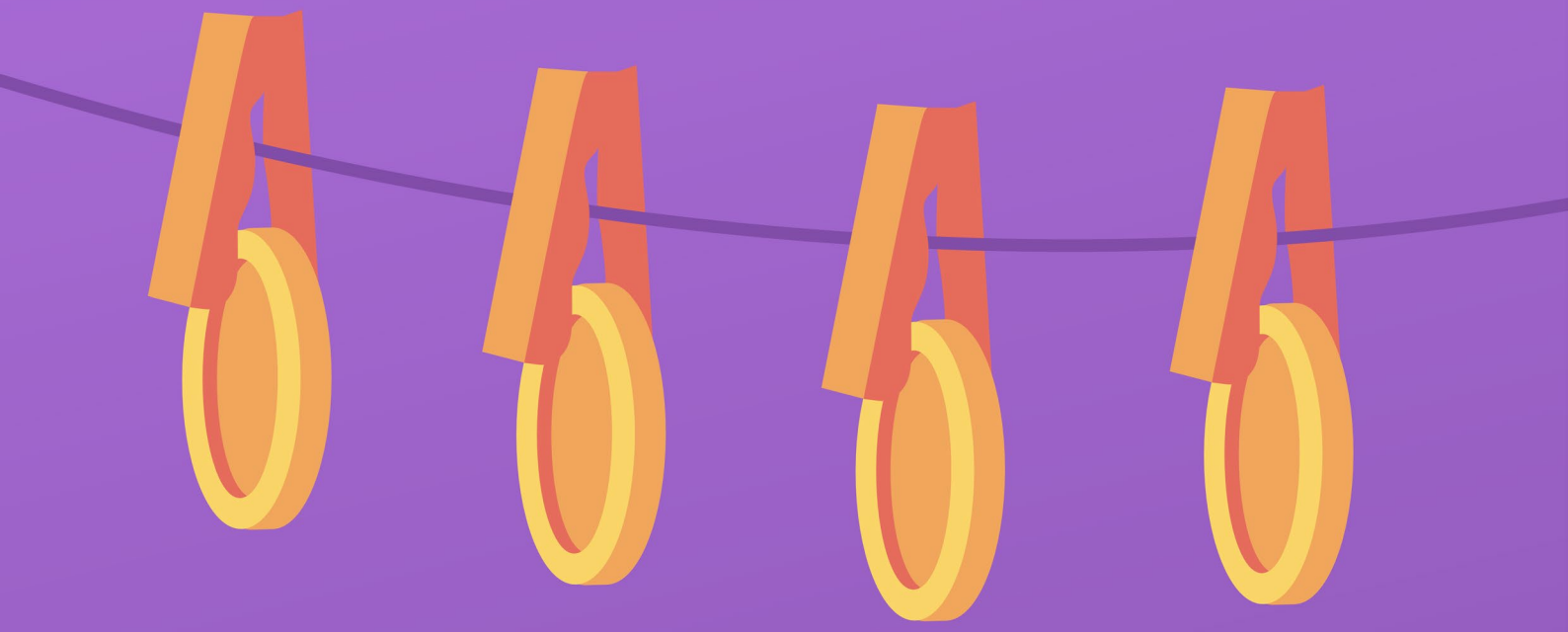
- Storing the digital currency in a cold wallet;
- Storing passwords, private keys, seed words, PINs, and digital currency addresses in text files within a dedicated folder for each seized digital currency on external storage devices, which must remain offline in a secure location until needed by law enforcement;
- Appointing a specific official to store the devices containing information such as passwords, private keys, seed words, PINs, and digital currency addresses and restricting access to these devices;
- Law enforcement may appoint a trusted Crypto Asset Physical Trader or Crypto Asset Storage Manager to manage the digital currency if law enforcement lacks reliable cybersecurity infrastructure for storing digital assets;

b **Converting the digital currency into fiat currency as soon as possible or within a certain period after the seizure is made.** If this mechanism is chosen for asset management, the regulation must include provisions granting law enforcement the authority to sell the digital currency, either directly or through a public auction, always aiming to maximize the sale value. The conversion may also be carried out through an agreement with a VASP specializing in digital currency exchange to convert the digital currency into fiat currency;

c Decisions regarding the actions to be taken on the digital currency are made **based on the written opinion of the digital currency owner,** indicating whether they prefer the digital currency to be kept in its original form or converted into fiat currency.

8

Given the number of parties that could be involved in the enforcement of digital currencies related to criminal offenses, strong cooperation and roles are needed from state institutions involved in the management and supervision of digital currencies, as well as law enforcement agencies, such as the National Cryptocurrency Enforcement Team (NCET) and Digital Asset Coordinator (DAC) Network in the United States. In Indonesia, this can be achieved by establishing cooperation or a special unit composed of authorities responsible for the enforcement of digital currencies related to criminal offenses, which should at least include the Financial Services Authority (OJK) as the authority responsible for regulating, managing, and supervising the trading of digital currencies, along with law enforcement agencies.



V.
CONCLUSION

A. Summary

The use of digital currencies is one of the consequences of the various efforts toward digitalization, which have targeted many sectors, including finance and banking. Cryptocurrency has become one of the digital currencies that has seen massive growth in terms of users and transaction value, both nationally and globally. The increasing use of cryptocurrencies is significantly influenced by their unique features, which offer various advantages, such as the ability to conduct transactions with global reach, fast and irreversible transactions, and the use of anonymous addresses and pseudonyms. However, at the same time, these unique characteristics of cryptocurrency also introduce certain risks. The reliance on fossil fuel energy, as well as the massive allocation of energy and resources required to support the blockchain technology that underpins cryptocurrency, leads to environmental damage and exacerbates the effects of the climate crisis. Additionally, cryptocurrencies also present risks of misuse in criminal activities, such as money laundering, fraud, and hacking.

The predicate crimes involving cryptocurrency are varied, ranging from drug trafficking, human trafficking, terrorism financing, to environmental crimes. In these various criminal activities, cryptocurrency as a digital currency can play different roles. It can serve as a payment tool and a means to facilitate the execution of crimes, conceal illicit financial activities, including as a means for money laundering by mining to create new digital-

coins using assets from illegal activities.

The vulnerability of cryptocurrency to misuse in criminal activities has indeed been addressed with the establishment of several regulations both internationally and in Indonesia. At the international level, general measures for preventing crimes involving digital currencies are outlined in FATF Recommendations No. 15 and 16 within the document on the Prevention and Combating of Money Laundering and Terrorism Financing. Meanwhile, in the enforcement domain, FATF in 2019 developed guidelines for the seizure, freezing, and confiscation of digital currencies, as outlined in the Guidance on Financial Investigations Involving Virtual Assets from 2019. Additionally, in 2021, FATF member countries in Latin America issued guidelines on the investigation, identification, seizure, and confiscation of digital currencies.

At the national level, the government's efforts to regulate the prevention and prosecution of crimes involving digital currencies have also become evident. This can be identified through the presence of several regulations that specifically target the rapidly expanding crypto assets or digital currencies. Among them is the Minister of Trade Regulation No. 99 of 2018 on General Policies for the Implementation of Crypto Asset Futures Trading, which was further detailed through two technical regulations, namely Bappebti Regulation No. 5 of 2019 and No. 7 of 2020. In the prevention mechanism, these regulations have incorporated key aspects of preventing the involvement of digital currencies in crimes, as outlined in FATF Recommendations No. 15 and 16. The series of Bappebti regulations implementing custodial wallets in Indonesia presents an opportunity to mitigate obstacles that may arise in the enforcement of crypto asset actions in the country.

Unlike the well-established preventive efforts through the creation of regulations mentioned above, the handling of criminal offenses involving cryptocurrencies, particularly the seizure of crypto assets in Indonesia, is still minimally regulated. Additionally, the lack of knowledge and experience among law enforcement officers regarding crypto assets and how to handle them also hinders the enforcement process. Currently, there is only one regulation related to the enforcement of crimes involving digital currencies, namely Attorney General's Guidelines No. 7 of 2023 on the Handling of Crypto Assets as Evidence in Criminal Cases. This regulation is considered insufficient, as it only binds law enforcement under the Attorney General's Office and does not regulate the seizure procedures for decentralized digital currencies.

B. Recommendations

The various conveniences and efficiencies offered by digital currencies must be accompanied by adequate efforts to mitigate the risks of misuse. Without such efforts, the sophistication and uniqueness of digital currencies, including cryptocurrencies, could ultimately turn into aspects that cause more harm than good. Therefore, we recommend several actions that are expected to contribute to the development and improvement of efforts to address crimes involving cryptocurrencies, including:

1. Incorporating provisions on the enforcement of digital currencies related to criminal offenses into the revision of the Indonesian Criminal Procedure Code (KUHAP). Specifically, this should regulate aspects related to seizure and/or blocking, including the planning, execution, and post-seizure stages, as well as other necessary enforcement actions such as searches, storage, and confiscation.

2. Expanding the scope of regulation to not only target centralized crypto assets but also decentralized crypto assets involved in criminal activities.

3. Enhancing the knowledge and technical skills of law enforcement officers regarding the intricacies of digital currencies and cryptocurrencies, including the handling mechanisms during the judicial process (searches, seizures, storage, confiscation, etc.), as well as understanding their vulnerabilities.

4. Intensive multi-stakeholder collaboration involving law enforcement personnel with expertise in intelligence, finance, and banking, as well as experts from actors within the crypto ecosystem such as, but not limited to, exchangers, trading platforms, and wallet providers.