Judul: Mengurai Kerentanan Penyalahgunaan dan Penindakan Mata Uang Digital yang Terkait dengan Tindak Pidana

Penulis:
Alia Yofira Karunian
Muhammad Aziezi Tanziel
Seira Tamara Herlambang

Pengulas:
Mawa Kresna

Editor:
Yassar Aulia
Egi Primayogha

Indonesia Corruption Watch
2024

Daftar Isi

I. Pendahuluan

Perkembangan teknologi berjalan semakin pesat dan berdampak pada munculnya berbagai inovasi digital. Kebaruan teknologi ini juga terjadi pada sektor keuangan dan perbankan melalui perubahan perilaku transaksi agen ekonomi ke arah digital. Salah satu contohnya adalah penggunaan mata uang kripto (*cryptocurrency*).

Aset kripto adalah mata uang digital yang menggunakan teknologi kriptografi untuk mengamankan transaksi. Kriptografi ini memastikan bahwa mata uang kripto tidak dapat dipalsukan atau digunakan secara ganda, sehingga pemiliknya dapat terhindar dari potensi kecurangan.[1] Dukungan teknologi yang disebut *blockchain* sebagai elemen tak terpisahkan dari kripto juga menjamin keamanan transaksi secara online meskipun tanpa adanya keterlibatan pihak ketiga. Banyak negara juga telah mengadopsi penggunaan kripto sebagai alternatif transaksi nontunai, seperti pengiriman uang lintas negara.[2] Beberapa negara seperti Belanda, Britania Raya, Jerman, Jepang, Amerika Serikat, dan Swiss bahkan telah mengakui dan memberi legitimasi terhadap penggunaan kripto sebagai mata uang.[3]

Antusiasme terhadap penggunaan kripto dari tahun ke tahun terus meningkat. Pada tataran global, jumlah pengguna kripto per November 2023 mencapai 420 juta orang dengan nilai kapitalisasi pasar mencapai US$1,41 triliun.[4] Sedangkan di tingkat domestik, Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti) mencatat sejak Februari 2021 jumlah pengguna di

[1] Dini Diah, "Mengenal Aset Kirpto: Pengertian, Kekurangan, dan Kelebihannya", *Tempo*, 25 Juli 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 Januari 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 Desember 2023, https://money.kompas.com/read/2023/12/22/170000726/jumlah-investor-kripto-di-indonesia-masuk-7-besar-dunia.

Indonesia meningkat rata-rata sekitar 437,9 ribu pelanggan setiap bulan.[5] Data teranyar menunjukan jumlah investor kripto di Indonesia pada Maret 2024 telah menyentuh angka 19,75 juta orang.[6] Sejalan dengan jumlah penggunanya yang terus bertambah, nilai transaksi kripto juga mengalami pertumbuhan signifikan. Dalam periode Januari sampai dengan Maret 2024 saja, nilai transaksi kripto di Indonesia mencapai Rp158,84 triliun.[7] Jumlah tersebut bahkan 4 kali lebih tinggi dari nilai transaksi pada periode bulan yang sama di tahun 2023.[8]

Meski kripto dilengkapi tingkat keamanan yang cukup tinggi sehingga dapat melindungi penggunanya, namun kripto sebagai sebuah komoditas tidaklah hadir tanpa risiko. Aset kripto juga memiliki kerentanan tinggi untuk disalahgunakan. Hal ini disebabkan transaksi melalui aset kripto dapat meningkatkan anonimitas sehingga menghambat pendeteksian aktivitas kejahatan oleh penegak hukum.[9] Karakteristik ini menyulitkan penelusuran terhadap pemilik aset kripto sebenarnya.[10] Celah inilah yang berpeluang disalahgunakan oleh pelaku tindak pidana untuk menyembunyikan atau menyamarkan aset hasil kejahatannya.

Kerentanan ini semakin tergambar lewat data pencucian uang lewat kripto di tingkat global cukup tinggi, yaitu mencapai US$8,6 miliar di tahun 2021. Nilai tersebut mencapai total US$33 miliar jika dikalkulasikan secara keseluruhan sejak tahun 2017 hingga 2021.[11] Di Indonesia juga sudah muncul beberapa kasus terkait dugaan pencucian uang lewat kripto. Misalnya, kasus korupsi PT Asuransi Sosial Angkatan Bersenjata Republik Indonesia (ASABRI) yang mana uang hasil korupsi diduga digunakan oleh para pelaku untuk membeli aset kripto. Serupa dengan kasus PT Asabri, ada pula kasus pencucian uang senilai

---

[5] Kementerian Perdagangan RI, "Bappebti Catat Pelanggan Aset Kripto Tembus 18,25 Juta", 18 Desember 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 Mei 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 Mei 2024, https://finance.detik.com/fintech/d-7337892/ojk-catat-transaksi-kripto-naik-hampir-rp-70-t-dalam-sebulan.

[8] *Ibid*

[9] Muh Afdal Yanuar, *op.cit.,* hal. 174.

[10] *Ibid*

[11] James Thorpe, "US$ 8.6 Billion Worth of Cryptocurrency Laundered by Cybercriminals in 2021", *International Security Journal*, 21 Februari 2022, https://internationalsecurityjournal.com/cryptocurrency-laundered-in-2021/

puluhan miliar oleh mantan pegawai Ditjen Pajak Kementerian Keuangan yang sebagian dari aset tersebut ditransaksikan untuk membeli kripto berupa Bitcoin.[12]

Pencucian uang bertujuan untuk menyembunyikan aset yang diperoleh secara ilegal agar seolah terlihat sebagai aset yang legal. Keunikan dan karakteristik kripto memiliki potensi untuk menjadi alat penyamaran aset dari sumber ilegal tersebut. Tindak pidana seperti korupsi, perdagangan narkotika dan psikotropika kerap menjadi kejahatan asal yang berisiko tinggi dalam penyalahgunaan kripto.[13] Tidak hanya itu, aset kripto juga memungkinkan menjadi tempat menyamarkan hasil tindak pidana lainnya seperti kejahatan lingkungan. Terlebih, Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) pada pertengahan 2023 juga sempat menemukan dugaan aliran dana ilegal termasuk pencucian uang terkait kejahatan di sektor lingkungan dengan jumlah fantastis yaitu senilai Rp20 triliun.[14]

Sejumlah penjabaran di atas semakin menunjukan pentingnya penelusuran lebih lanjut terhadap potensi penyalahgunaan kripto dalam menyamarkan aset hasil tindak pidana dan penanggulangan yang bisa dilakukan terhadapnya. Laporan ini akan mengulas tentang *status quo* pengaturan, praktik pencegahan serta penindakan kejahatan yang melibatkan kripto. Selain itu, laporan ini juga akan membahas mengenai tantangan dan peluang dalam memperbaiki upaya pencegahan dan penindakan yang sudah ada.

[12] "Rafael Cuci Uang Miliaran Pakai Bitcoin, Ini kata PPATK!", *CNBC Indonesia,* 12 Mei 2023, https://www.cnbcindonesia.com/news/20230512113504-4-436827/rafael-cuci-uang-miliaran-pakai-bitcoin-ini-kata-ppatk.
[13] Muh Afdal Yanuar, *loc.cit.*
[14] Rahel Narda Chaterine, dan Sabrina Asril, "PPATK: Pencucian Uang Terkait Kejahatan Lingkungan Sampai Rp20 Triliun", *Kompas,* 27 Juni 2023, https://nasional.kompas.com/read/2023/06/27/16081621/ppatk-pencucian-uang-terkait-kejahatan-lingkungan-sampai-rp-20-triliun

II. Mengenal Teknologi *Blockchain* dan *Cryptocurrency*

A. *Blockchain*

Asal muasal penamaan teknologi *blockchain* atau rantai blok memiliki keterkaitan dengan cara teknologi ini menyimpan data transaksi, yakni di dalam sebuah blok (*block*) yang dihubungkan bersama lalu membentuk rantai (*chain*).[15] Gagasan inti *blockchain* pertama kali mengemuka pada akhir tahun 1980-an dan awal 1990-an, sebagai sebuah protokol bernama "*Paxos Protocol*" yang digagas oleh Leslie Lamport.[16] Pada tahun 2008, *blockchain* kemudian mulai dikenal luas sebagai teknologi yang mendasari *cryptocurrency*, Bitcoin, yang digagas oleh seseorang (atau sekelompok orang) yang dikenal dengan pseudonim Satoshi Nakamoto.[17] Satoshi bervisi bahwa di masa depan transaksi uang antar pihak akan dicatat dalam sebuah buku besar bersama, dikelola oleh komputer yang tersebar di seluruh dunia (jaringan "*nodes*").[18]

Selaras dengan visi Satoshi, Tran dan Krishnamachari (2022) kemudian mendefinisikan *blockchain* secara teknis sebagai "sistem komputasi terdesentralisasi yang terdiri dari lima komponen penyusunnya: jaringan terdesentralisasi, kriptografi matematika, konsensus terdistribusi, buku besar transaksi, dan kontrak cerdas".[19] Adapun penjelasan lebih lanjut terkait lima komponen tersebut, *inter alia*:

Tabel 1: Komponen-Komponen Teknologi *Blockchain*

[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.

Komponen *Blockchain*	Keterangan
Jaringan Terdesentralisasi	*Blockchain* merupakan jaringan komputer terdesentralisasi (disebut sebagai *node*), yang kemudian menjadi sumber daya komputasi untuk membantu menyimpan dan memproses transaksi.
Kriptografi Matematika	*Blockchain* menggunakan metode kriptografi yang juga berfungsi untuk membuktikan bahwa secara matematis, *blockchain* berfungsi sebagaimana mestinya. Lebih lanjut, *blockchain* menggunakan *hash* kriptografi guna menghubungkan blok data (*block*) dalam rantai (*chain*) untuk mencegah terjadinya perubahan data setelah perekaman blok data baru dalam sistem *blockchain* (*immutability*).
Konsensus Terdistribusi	Untuk menentukan sah atau tidaknya suatu transaksi, tidak ada otoritas pusat yang memutuskan. Sebaliknya, keputusan tersebut diambil berdasarkan konsensus yang dicapai di antara jaringan *nodes* yang berpartisipasi. Saat ini ada dua ragam mekanisme konsensus (*mechanism of consensus*) yang biasa digunakan dalam sistem *blockchain*, yakni *proof-of-work* (POW) dan *proof-of-stake* (POS).
Buku Besar Transaksi	*Blockchain* merupakan buku besar digital yang menyimpan transaksi secara kronologis dalam blok-blok yang ditambahkan terhadap data yang sudah ada (*append-only*). Hal ini merupakan struktur data yang mendasari bagaimana buku besar untuk hampir semua jaringan *blockchain* bekerja.
Kontrak Cerdas (*Smart Contract*)	Aplikasi yang menggunakan teknologi *blockchain* diimplementasikan sebagai *smart contract* atau kontrak cerdas, sebuah istilah yang diciptakan oleh Nick Szabo pada tahun 1994.[20] Kontrak cerdas berbeda dengan kontrak pada umumnya, karena pelaksanaannya yang bersifat otomatis, tanpa campur tangan manusia.

[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.

(Sumber: Handbook on Blockchain, 2022)

Lebih lanjut, Tran dan Krishnamachari (2022) juga menggarisbawahi setidaknya tiga karakteristik yang membuat teknologi *blockchain* berbeda, yakni "aman (tidak ada kemungkinan kehilangan atau perubahan data), transparan (verifikasi dan penelusuran mudah), dan *trustless* (kepercayaan transaksi tanpa perantara)".[21]

Berdasarkan pembatasan izin bagi jaringan *nodes* untuk menambahkan data ke sistem *blockchain*, teknologi *blockchain* dapat diklasifikasikan menjadi dua jenis, yakni *Blockchain Permissionless* (jaringan *nodes* tidak memerlukan izin untuk berpartisipasi) dan *Permissioned* (jaringan *nodes* terlebih dahulu memerlukan izin untuk berpartisipasi).[22] Lebih lanjut, berdasarkan pada siapa yang dapat mengakses dan melihat buku bersama *blockchain*, *blockchain* juga dapat dikategorikan sebagai publik (terbuka untuk siapapun untuk melihat) atau privat (hanya dapat diakses oleh peserta jaringan node yang telah diberikan persetujuan sebelumnya).[23]

Teknologi *blockchain* digadang-gadang lebih unggul dibandingkan dengan teknologi lainnya yang mengadopsi pendekatan sentralisasi, khususnya dalam empat aspek krusial yakni: kepercayaan, keamanan, privasi, dan transparansi.[24] Meskipun demikian, tak sedikit pihak yang menyuarakan permasalahan teknologi *blockchain* di empat aspek krusial ini. Suripeddi dan Purandare (2021) misalnya, keduanya menggarisbawahi bagaimana dampak negatif pemanfaatan *blockchain* terhadap hak atas privasi, khususnya terkait perlindungan data pribadi pengguna *blockchain*.[25] Selain itu, hasil studi yang dilakukan Tuyisenge (2021) juga menemukan bahwa dalam teknologi *blockchain* tidak luput dari serangan keamanan digital. Tuyisenge mengidentifikasi sebanyak 51% serangan keamanan mengakibatkan pembelanjaan ganda (*double spending*) dan pendapatan tidak adil (*unfair income*), sedangkan serangan terhadap *wallet software* mengakibatkan eksekusi kode tidak sah

[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," *Journal of Physics: Conference Series* 1964, no. 4 (July 2021): 11, https://doi.org/10.1088/1742-6596/1964/4/042005.

(*unauthorized code execution*), penolakan layanan (*denial of service*), dan kebocoran *private key* pengguna.[26]

Hal lainnya yang juga disoroti terkait pemanfaatan teknologi *blockchain* adalah dampaknya terhadap lingkungan, khususnya terkait konsumsi energi yang dibutuhkan untuk menopang teknologi *blockchain*. Dalam sistem *blockchain* yang menggunakan mekanisme konsensus POW misalnya, proses penambangan yang dilakukan mengkonsumsi daya listrik dengan jumlah yang sama dengan konsumsi daya listrik yang dibutuhkan negara Swiss dalam setahun.[27] Secara spesifik, berbagai studi yang khusus mempelajari dampak lingkungan dari proses penambangan Bitcoin (salah satu jenis kripto) sangat bergantung pada energi fosil. [28] Sebanyak 67% dari listrik yang digunakan untuk penambangan Bitcoin di tahun 2020 sampai dengan 2021 dihasilkan dari sumber energi fosil. Dari angka penggunaan energi fosil tersebut, batu bara mendominasi sumber penyediaan listrik yang digunakan untuk penambangan Bitcoin sebesar 45% secara global pada periode yang sama.[29]
Di sisi lain, berbagai upaya telah dilakukan guna menekan dampak lingkungan dari proses penambangan Blockchain. Sebuah studi yang dilakukan pada tahun 2023 mengidentifikasi setidaknya 23 jaringan *blockchain* yang mengonsumsi daya jauh lebih sedikit dan memproduksi lebih sedikit emisi karbon dioksida dibandingkan dengan jaringan Bitcoin.[30] Meski demikian, Bitcoin masih menjadi jenis blockchain yang mendominasi pasar kripto di Indonesia. Pada 2024, Bappebti mencatat Bitcoin menguasai lebih dari separuh total kapitalisasi pasar aset kripto di Indonesia.[31]

Penggunaan dan ketergantungan yang besar atas energi khususnya yang berasal dari batu bara dalam proses penambangan jaringan *blockchain,* khususnya Bitcoin, berpotensi menghasilkan kerusakan lingkungan sebagai dampak yang tak terhindarkan. Oleh karena itu, ketika menganalisis efisiensi biaya dari teknologi

[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.
[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 Oktober 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 Februari 2024, https://www.kemendag.go.id/berita/pojok-media/bappebti-targetkan-transaksi-kripto-rp800-triliun-pada-2024.

blockchain, penting juga untuk memperhitungkan dampak lingkungan sebagai faktor penentu.

B. Mata Uang Kripto (Cryptocurrency): 101

Pada tahun 2023, Indonesia menduduki peringkat ke-6 negara dengan kepemilikan mata uang kripto tertinggi di dunia.[32] Peringkat yang cukup tinggi ini digapai Indonesia, meski terjadi penurunan tajam volume transaksi aset kripto di Indonesia sebanyak 63% pada tahun 2022.[33] Terlepas terjadi penurunan pasar mata uang kripto secara global, [34] Chainalysis, sebuah perusahaan yang berfokus pada analisis *blockchain* dan penyedia layanan investigasi kripto, mencatat bahwa terdapat peningkatan volume transaksi gelap kripto selama dua tahun berturut-turut, yang pada tahun 2022 mencapai angka tertinggi sepanjang masa sebesar US$20,6 miliar.[35] Lebih lanjut lagi, Chainalysis juga menemukan bahwa besaran mata uang kripto yang merupakan hasil pencucian uang meningkat 68% pada tahun 2022.[36] Pemerintah Indonesia telah jauh mengidentifikasi penggunaan mata uang kripto, Bitcoin, sebagai bentuk ancaman terkini tindak pidana pencucian uang sejak tahun 2015.[37]

Lantas apa itu mata uang kripto atau yang kerap dikenal sebagai *cryptocurrency*? Sebuah studi yang dilakukan *European Parliament* (Parlemen Eropa) menunjukkan bahwa dalam konteks regulasi, tidak ada definisi *cryptocurrency* yang disepakati bersama. Berbagai institusi perbankan dan finansial dunia mengkategorisasikan *cryptocurrency* sebagai bagian dari mata uang digital atau virtual.[38] Parlemen Eropa mendefinisikan *cryptocurrency* sebagai "representasi nilai digital yang (i) dimaksudkan sebagai alternatif *peer-to-peer* ("P2P") terhadap alat pembayaran sah yang dikeluarkan pemerintah, (ii) digunakan sebagai media pertukaran untuk tujuan umum (terlepas dari lembaga perbankan pusat manapun), (iii) dijamin dengan mekanisme yang disebut kriptografi dan (iv) dapat dikonversi menjadi alat

[32] "The State of Crypto & NFTs in 2023," DataReportal – Global Digital Insights, 28 Januari 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 Januari 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, Juli 2018), 20–23, https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2018)619024.

pembayaran yang sah dan sebaliknya".[39] Dalam kajian yang sama, terdapat beberapa aktor yang dapat diidentifikasi dalam ekosistem jual beli *cryptocurrency*. Adapun aktor-aktor tersebut, *inter alia*:[40]

Tabel 2: Aktor-Aktor dalam Ekosistem *Cryptocurrency*

Aktor	Peran
Pengguna (*User*)	Orang perseorangan atau badan hukum yang mendapatkan koin untuk menggunakannya untuk (i) membeli barang atau jasa nyata atau virtual (dari sekumpulan pedagang tertentu), (ii) untuk melakukan pembayaran *Peer-to-Peer*, atau (iii) untuk menyimpannya untuk tujuan investasi. Setiap pengguna dalam jaringan *blockchain* memiliki dua kunci: (i) *private key* (kunci privat), yang digunakan untuk membuat tanda tangan digital dalam sebuah transaksi, dan (ii) *public key* (kunci publik), yang diketahui oleh seluruh aktor-aktor lainnya dalam jaringan *blockchain*.[41]
Penambang (*Miner*)	Penambang terdiri dari pengguna (*user*) atau pihak lainnya yang memang mencari keuntungan dari proses penambangan *cryptocurrency* untuk kemudian ditukarkan dengan mata uang fiat. Para penambang berpartisipasi dalam proses validasi transaksi dalam sistem *blockchain* dengan melakukan *puzzle* kriptografi. Proses penambangan ini khususnya terkait pada *cryptocurrency* yang menggunakan mekanisme konsensus POW.
Tempat penukaran mata uang kripto (*cryptocurrency exchanges*)	Tempat penukaran mata uang kripto adalah badan hukum yang menawarkan layanan penukaran mata uang kripto bagi pengguna, biasanya untuk pembayaran biaya tertentu. Layanan yang ditawarkan dapat berupa layanan penukaran mata uang kripto untuk menjual koin mereka dengan mata uang fiat, atau sebaliknya, membeli koin baru dengan mata uang fiat.

[39] Houben and Snyers, 23.
[40] Houben and Snyers, 25–28.
[41] Houben and Snyers, 16.

Platform Jual Beli (*trading platforms*)	Platform jual beli mata uang kripto adalah sebuah *marketplaces* yang mempertemukan para pengguna mata uang kripto dengan satu sama lain sehingga mereka dapat melakukan jual beli secara langsung (sebagai contoh, sebuah "eBay" bagi pengguna mata uang kripto).
Penyedia Layanan Dompet Mata Uang Kripto (*wallet providers*)	Penyedia layanan dompet mata uang kripto adalah pihak yang menyediakan layanan dompet digital kepada pengguna mata uang kripto, guna menyimpan dan mentransfer koin dengan mudah.
Pembuat Koin (*coin inventors*)	Pembuat koin adalah individu atau organisasi yang mengembangkan pondasi teknis dari mata uang kripto dan menentukan aturan awal penggunaan mata uang kripto tersebut. Dalam beberapa kasus pembuat koin diketahui identitasnya (misalnya, Ethereum, Ripple, Litecoin, Cardano), namun di beberapa kasus lainnya, identitas pembuat koin mata uang kripto tidak diketahui (misalnya, Bitcoin dan Monero).
Pemberi Koin (*coin offerors*)	Pemberi koin adalah individu atau organisasi yang menawarkan koin mata uang kripto kepada para pengguna setelah rilisnya koin tersebut, untuk biaya tertentu atau secara gratis. Pemberi koin juga dapat merupakan pihak yang sama dengan Pembuat Koin, atau juga individu atau organisasi yang terpisah.

(Sumber: *Cryptocurrencies and Blockchain*, 2018)

Tempat penukaran mata uang kripto (*cryptocurrency exchanges*), sebagai tempat pengguna dapat menukarkan koin mata uang kripto menjadi mata uang fiat, menjadi aktor penerima terbesar mata uang kripto ilegal.[42] Selain *cryptocurrency exchanges*, pihak lainnya yang juga memfasilitasi pencucian uang mata uang kripto adalah penyedia layanan dompet mata uang kripto (*wallet providers*). Dalam sebuah studi yang dilakukan oleh Transparansi Internasional Rusia (2023), ditemukan bahwa terdapat perantara di *dark web* yang menawarkan akun *money mule* di Wirex dengan biaya tertentu.[43] Akun-akun *money mule* ini pada umumnya terdaftar atas nama warga negara atau pengungsi yang memiliki izin tinggal di negara-negara seperti

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

Ukraina, Latvia, Estonia, Polandia, Republik Ceko, Bulgaria, dan Spanyol.[44] Para penjual akun *money mule* ini juga menyanggupi penjualan akun dalam jumlah besar, yang kemudian membuka peluang terjadinya *smurfing* (sebuah praktik pencucian uang dengan cara memecah uang besar dalam beberapa transaksi yang lebih kecil untuk menghindari pengawasan pencucian uang).[45]

Oleh karena itu, upaya mengatur transaksi mata uang kripto haruslah menyasar aktor-aktor berisiko tinggi, yakni Tempat Penukaran mata uang kripto (*cryptocurrency exchanges*), Platform Jual Beli (*trading platforms*) dan Penyedia Layanan Dompet Mata Uang Kripto (*wallet providers*). Pada praktiknya, satu perusahaan dapat berperan ganda dan menawarkan lebih dari satu dari ketiga layanan di atas. Sebagai contoh, pedagang aset fisik kripto, INDODAX, juga menawarkan layanan penukaran (*cryptocurrency exchanges*) dan dompet (*wallet providers*) mata uang kripto.[46] Selain itu itu, penting untuk memahami lebih lanjut mengenai beragam model bisnis dari *wallet providers*, yang sangat berdampak pada upaya untuk menanggulangi tindak pidana yang melibatkan mata uang kripto. *Wallet providers* pada dasarnya terbagi berdasarkan bagaimana mereka menyimpan kunci (publik dan privat) pengguna yang digunakan untuk melakukan validasi transaksi mata uang kripto. Secara garis besar, *wallet providers* terbagi menjadi kelompok-kelompok berikut:

1. **Berdasarkan apakah pengguna memiliki kontrol penuh atas *private key*.** Berdasarkan kriteria ini, *wallet providers* terbagi menjadi dua, yakni: *non-custodial* (dikenal juga sebagai '*unhosted wallet*') dan *custodial wallet* (dikenal juga sebagai '*hosted wallet*').[47] Adapun perbedaan karakteristik di antara keduanya adalah sebagai berikut:[48]

Tabel 3: Perbedaan *Custodial* dan *Non-Custodial Wallet*

Custodial Wallet	Non-Custodial Wallet
1. Pengguna *custodial wallet* tidak memiliki kontrol penuh	1. Pengguna *non-custodial wallet* memiliki kontrol penuh

[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/.
[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/.

2. *Private key* pengguna disimpan oleh pihak ketiga (*centralized*) **3.** *Private* key tersedia secara *online*	2. *Private key* disimpan hanya oleh pengguna (*decentralized*) 3. *Private key* tersedia secara *online* dan *offline*

2. **Berdasarkan apakah *wallet* terhubung ke internet atau tidak.** Berdasarkan kriteria ini, *wallet providers* terbagi menjadi dua, yakni: *hot* dan *cold wallet*.[49] Adapun perbedaan karakteristik di antara keduanya adalah sebagai berikut:[50]

Tabel 4: Perbedaan Hot dan Cold Wallet

Hot Wallet	Cold Wallet
1. Terhubung ke internet secara terus menerus **2.** Dompet Virtual **3.** Jenis: Desktop, Mobile, atau Hybrid (kombinasi keduanya)	1. Tidak terhubung ke internet secara terus menerus 2. Dompet Virtual dan Fisik 3. Jenis: *Hardware* (misal: USB) atau Kertas (misal: kode QR)

[49] European Central Bank, *Virtual Currency Schemes: A Further Analysis* (LU: European Central Bank, 2015), 8, https://data.europa.eu/doi/10.2866/662172.
[50] 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. Pengaturan dan Praktik Pencegahan dan Penindakan Kejahatan yang Melibatkan Mata Uang Digital

A. Gambaran Umum Kejahatan yang Melibatkan Mata Uang Digital

Dalam beberapa tahun terakhir, mata uang digital telah berkembang menjadi salah satu mekanisme pembayaran yang dibangun berdasarkan sistem atau protokol perangkat lunak dari mata uang digital tersebut. Mekanisme pembayaran ini berupaya menyediakan metode baru untuk mengirimkan suatu nilai tertentu melalui internet. Namun, pada saat yang sama, produk dan layanan pembayaran mata uang digital menimbulkan risiko terjadinya kejahatan pencucian uang, pendanaan terorisme, serta kejahatan lainnya yang harus diidentifikasi dan dimitigasi.[51]

Saat ini, para pelaku kejahatan semakin banyak mengeksploitasi aset atau mata uang digital seiring dengan semakin meluasnya penggunaan mata uang digital, salah satunya kripto yang semakin terdiversifikasi dengan cepat. Terkait hal tersebut, *U.S. Department of Justice* (Departemen Kehakiman AS) dalam dokumen *The Cryptocurrency Enforcement Framework*[52] mengkategorikan bentuk-bentuk hubungan mata uang digital dengan kejahatan sebagai berikut:[53]

(1) Mata uang digital sebagai alat pembayaran atau cara memfasilitasi pelaksanaan kejahatan

Dalam beberapa kasus, ditemukan bahwa mata uang digital digunakan untuk membeli dan menjual obat-obatan terlarang, untuk menyebarkan iklan dan mempromosikan perdagangan manusia, menjadi pilihan metode dan pengumpulan pembayaran *ransomware*[54] dan aktivitas pemerasan digital lainnya, untuk melakukan penipuan dan pencurian terhadap konsumen dan investor, dan untuk membiayai ancaman terhadap keamanan nasional, termasuk penggalangan dana kegiatan terorisme. Hal ini dilakukan

---

[51] The Financial Action Task Force (FATF), *Guidance for a Risk-based Approach: Virtual Currencies*, (Paris: FATF, 2015), hal. 3.

[52] *The Cryptocurrency Enforcement Framework* adalah dokumen yang menjelaskan prosedur hukum yang tersedia untuk memproses hukum penggunaan mata uang digital secara illegal, menjabarkan profil, peran, dan tanggung jawab badan/lembaga pemerintah dalam bidang aset digital, dan menguraikan strategi untuk mengatasi ancaman yang muncul terhadap keamanan dan pengoperasian pasar mata uang digital yang efektif. Lihat 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), hal. 14.

[53] *Ibid.*, hal. 4 – 9.

[54] *Ransomware* adalah sejenis *malware* atau virus yang dimasukkan pelaku ke dalam sistem komputer milik korban dan mengunci data di dalam komputer dimana pelaku *ransomware* akan meminta tebusan pada korbannya jika data yang dikunci ingin dibuka. Umumnya, tebusan tersebut tidak menggunakan mata uang yang umum digunakan, melainkan berupa mata uang virtual Bitcoin. Selain itu, virus ini juga dapat mengunci seluruh sistem, sehingga jalan satu-satunya adalah dengan membayar uang tebusan yang diminta untuk dapat menggunakan komputernya kembali. Lihat Badan Aksesibilitas Telekomunikasi dan Informasi, "Ciri-Ciri Komputer Terinfeksi Ransomware & Cara Mengatasinya", https://www.baktikominfo.id/id/informasi/pengetahuan/ciri-ciri_komputer_terinfeksi_ransomware_cara_mengatasinya-750, diakses pada Kamis, 15 Februari 2024.

oleh para pelaku kejahatan dengan memanfaatkan sifat anonimitas pada mata uang digital sehingga dapat menutupi identitas asli dari para pelaku tersebut. Bahkan, pada tahun 2021, *Federal Bureau Investigation* (FBI) Amerika Serikat menerima 3.729 pengaduan terkait *ransomware* melalui Pusat Pengaduan Kejahatan Internet dengan kerugian yang nilainya lebih dari US$49,2 juta;

(2) Penggunaan mata uang digital sebagai sarana untuk menyembunyikan aktivitas keuangan terlarang (*illicit*)

Selain sebagai alat pembayaran suatu kejahatan, pelaku kejahatan dalam beberapa kasus lain juga menggunakan mata uang digital untuk melakukan kejahatan pencucian uang dan memfasilitasi penghindaran pajak. Di samping memanfaatkan sifat anonimitas, para pelaku kejahatan tersebut juga mengandalkan teknik pengaburan yang semakin canggih, seperti transaksi yang rumit dan cepat, melakukan "*chain hopping*" dengan mengubah dana dari satu mata uang digital ke mata uang digital lainnya, dan tindakan lainnya yang dirancang untuk mempersulit penelusuran dan membuat uang digital tersebut tidak dapat dipulihkan. Kejahatan-kejahatan ini menjadi lebih mudah dilakukan karena banyak *platform* dan bursa mata uang digital yang tidak berupaya untuk mematuhi peraturan anti pencucian uang, seperti persyaratan "*Know Your Customer*" (KYC) atau beroperasi di yurisdiksi yang tidak memiliki aturan-aturan anti pencucian uang dan persyaratan pemberantasan pendanaan yang sejalan dengan standar internasional;

(3) Kejahatan yang melibatkan atau mempengaruhi ekosistem mata uang digital

Seiring dengan meningkatnya minat terhadap penggunaan mata uang digital yang telah menciptakan peluang pasar yang signifikan, muncul pula pelaku-pelaku kejahatan yang menargetkan ekosistem mata uang digital, seperti pencurian mata uang digital, penipuan dengan hasil kejahatan berupa mata uang digital, hingga kejahatan dengan teknologi khusus seperti *crypto jacking*, yaitu penggunaan komputer milik orang lain secara tidak sah untuk menambang mata uang digital. Menurut perkiraan dari perusahaan analisis *blockchain*, terdapat lebih dari US$3,2 miliar mata uang digital yang dicuri, baik dari individu, maupun layanan mata uang digital pada tahun 2021. Contoh kasus pencurian mata uang digital adalah kasus Grup Lazarus pada bulan Maret 2022 yang mencuri mata uang digital senilai lebih dari US$600 juta dari *platform* game *online* dan pencurian mata uang digital senilai US$ 8 miliar yang dilakukan oleh pendiri bursa mata uang kripto FTX, Sam Bankman-Fried, pada bulan November 2022.[55]

Untuk kasus pencucian uang, pelibatan mata uang digital dalam kejahatan tersebut telah terjadi pada beberapa kasus, antara lain:

1. Di Inggris, *London Metropolitan Police* berhasil melakukan penyitaan terhadap kripto senilai £180,000,000 pada Juli 2021 dan U.K.'s National Crime Agency (NCA) yang berhasil merampas mata uang kripto/digital senilai £26,900,000 dalam rentang waktu 1

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

April 2021 – 31 Maret 2022. Dua kasus penyitaan tersebut diduga terkait dengan kejahatan pencucian uang;[56]

2. Kasus "*Silk Road*" di Amerika Serikat pada tahun 2013-2014. Dalam kasus itu Departemen Kehakiman AS berhasil menyita situs web *Silk Road* (sebuah situs web tersembunyi yang dirancang untuk memungkinkan penggunanya melakukan transaksi jual beli narkotika, senjata, informasi identitas curian, peretasan komputer (*hacking*), dan pencucian uang) serta menyita 173.991 Bitcoin senilai £33,600,000 di *Silk Road* dari perangkat komputer yang disita;[57]
3. Kasus perusahaan bursa mata uang kripto Binance di Amerika Serikat yang didakwa melanggar undang-undang anti pencucian uang Amerika Serikat karena memproses transaksi keuangan terkait berbagai aktivitas kejahatan. Dalam kasus tersebut, pendiri Binance, Changpeng Zhao, mengaku bersalah atas kejahatan tersebut dan dijatuhi hukuman 4 bulan penjara, denda sebesar US$ 50 juta, dan harus mengundurkan diri dari jabatan CEO Binance oleh pengadilan. Pengadilan juga menjatuhi hukuman kepada Binance sebagai perusahaan dengan denda sebesar US$ 4,3 miliar.[58]

Merespon kejahatan-kejahatan tersebut, *The Financial Action Task Force* (FATF)[59] mengungkapkan bahwa kejahatan-kejahatan yang melibatkan mata uang digital terjadi karena para pelakunya dapat memanfaatkan fitur-fitur unik dari mata uang digital, seperti penyelesaian transaksi yang cepat dan tidak dapat diubah, serta penggunaan alamat dan nama samaran. Kondisi ini kemudian diperburuk dengan semakin berkembangnya pasar *online* mata uang digital ilegal, seperti *Silk Road* dan *Alphabay*, yang seringkali di-*hosting* secara anonim di "*darknet*", yaitu bagian Internet yang tidak diindeks oleh mesin pencari dan memerlukan perangkat lunak khusus untuk mengaksesnya. FATF kemudian menjabarkan beberapa faktor yang membuat mata uang digital memiliki potensi risiko untuk digunakan dalam kejahatan seperti pencucian uang dan pendanaan terorisme, antara lain:[60]

1. Penggunaan mata uang digital memungkinkan anonimitas yang lebih besar dibandingkan dengan metode pembayaran non-tunai tradisional. Mata uang digital dapat diperdagangkan di Internet, umumnya ditandai dengan hubungan pelanggan non-tatap

---

[56] 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

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

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

[59] *The Financial Action Task Force* (FATF) adalah badan antar pemerintah yang berfungsi sebagai *watchdog* dalam pencegahan dan penindakan kejahatan pencucian uang dan pendanaan teroris global. Untuk melakukan itu, FATF menetapkan standar internasional yang bertujuan untuk mencegah aktivitas ilegal ini dan kerugian yang ditimbulkannya terhadap masyarakat. Lihat profil FATF di https://www.fatf-gafi.org/en/the-fatf/who-we-are.html , diakses pada Kamis, 15 Februari 2024. Indonesia telah menjadi anggota FATF ke-40 sejak 27 Oktober 2023. Lihat Kementerian Keuangan RI, "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 , diakses pada Kamis, 15 Februari 2024.

[60] FATF, *Guidance for a Risk-based Approach: Virtual Currencies …, Op. Cit.,* hal. 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.

muka, dan membuka kesempatan pendanaan secara anonim, yaitu pendanaan tunai atau pendanaan pihak ketiga melalui penukaran virtual yang tidak mengidentifikasi sumber pendanaan dengan tepat. Metode ini juga memberikan peluang dilakukannya transfer secara anonim walaupun pihak pengirim dan penerima tidak teridentifikasi secara memadai;

2. Sifat anonimitas tersebut semakin membuat mata uang digital rentan disalahgunakan akibat sistem perdagangannya yang terdesentralisasi yang tidak memiliki server atau penyedia layanan terpusat untuk mata uang digital. Misalnya pada Bitcoin, alamat Bitcoin yang berfungsi sebagai akun tidak memiliki nama atau metode identifikasi lainnya dan protokol Bitcoin tidak menghasilkan catatan sejarah transaksi yang harus dikaitkan dengan identitas pihak yang bertransaksi di dunia nyata. Akibat tidak adanya server terpusat sebagai badan pengawas dan belum adanya perangkat lunak pencegahan pencucian uang guna memantau dan mengidentifikasi pola transaksi mencurigakan, penegak hukum tidak dapat dengan mudah menargetkan satu lokasi atau entitas pusat (administrator) untuk tujuan investigasi atau penyitaan ketika Bitcoin tersebut disalahgunakan;
3. Transaksi mata uang digital dapat dilakukan melalui internet dengan jangkauan global (lintas batas negara). Belum lagi, transaksi mata uang digital biasanya melibatkan beberapa entitas yang seringkali berada pada lokasi/yurisdiksi yang berbeda-beda, termasuk di tempat-tempat yang tidak memiliki mekanisme pencegahan pencucian uang/pendanaan terorisme yang memadai. Hal ini menyebabkan ketidakjelasan pihak yang perlu bertanggung jawab atas kepatuhan dan pengawasan/penegakan aturan-aturan anti pencucian uang/pendanaan terorisme dan menyulitkan penegak hukum dan regulator untuk mengakses data-data transaksi mata uang digital, terlebih dengan sifat anonimitas dan desentralisasi.

Masalah anonimitas dalam transaksi mata uang digital di atas juga diyakini oleh Parlemen dan Dewan Uni Eropa sebagai hal yang meningkatkan potensi penyalahgunaan mata uang digital untuk tujuan kejahatan. Parlemen dan Dewan Uni Eropa menambahkan bahwa adanya entitas yang terlibat sebagai layanan pertukaran antara mata uang virtual dan mata uang fiat serta penyedia dompet kustodian tidak akan sepenuhnya mengatasi masalah anonimitas yang melekat pada transaksi mata uang digital. Hal ini disebabkan transaksi mata uang virtual tetap dapat dilakukan secara anonim ketika para pengguna bertransaksi tanpa penyedia tersebut. Untuk mengurangi risiko dari anonimitas tersebut, *Financial Intelligence Unit* (FIU) harus dapat memperoleh informasi yang memungkinkan FIU untuk mengaitkan alamat mata uang digital dengan identitas pemilik mata uang digital tersebut.[61]

B. Kejahatan Lingkungan dan Pelibatan Mata Uang Digital

[61] 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 Mei 2018, par. 9

Merujuk pada *United Nations Environment Programme* (UNEP) dan INTERPOL, kejahatan lingkungan digambarkan sebagai kegiatan ilegal yang merusak lingkungan dan bertujuan untuk menguntungkan individu, kelompok, dan/atau perusahaan dari eksploitasi, perusakan, perdagangan, atau pencurian sumber daya alam yang termasuk namun tidak terbatas pada kejahatan serius dan kejahatan terorganisir transnasional.[62] Adapun kegiatan ilegal dalam kejahatan lingkungan mencakup kejahatan terhadap satwa liar, kejahatan polusi, perdagangan bahan kimia terlarang, penangkapan ikan dan penambangan ilegal, serta pembalakan liar.

Saat ini, kejahatan lingkungan sudah berada pada tingkat yang memprihatinkan. Pada tahun 2021 kejahatan lingkungan bahkan telah masuk ke dalam tiga besar kejahatan global dengan nilai keuntungan ilegal mencapai US$281 miliar.[63] Situasi ini tentunya sangat mengkhawatirkan, sebab kejahatan lingkungan memiliki implikasi yang tidak hanya menyangkut kerusakan dan kelangkaan sumber daya alam, terganggunya kesehatan manusia, hingga terhambatnya pembangunan sosial-ekonomi.[64] Baik alam maupun kehidupan masyarakat sama-sama harus menanggung akibat dari kejahatan lingkungan. Dalam lingkup kehidupan masyarakat, kejahatan lingkungan dapat memberi keuntungan pada kelompok bersenjata dan memicu konflik keamanan.

Kejahatan lingkungan memiliki karakter yang serupa dengan perdagangan narkotika dan perdagangan orang. Kejahatan tersebut dilakukan melewati lintas batas negara dan karenanya tergolong dalam kategori kejahatan transnasional. Sebagai contoh, pelaksanaan aktivitas eksploitasi, keberadaan penadah, dan lokasi pencucian uang hasil kegiatan ilegal, berada di negara yang berbeda-beda. Pada akhirnya, kejahatan lingkungan juga bermuara pada kejahatan lain berupa pencucian uang dan pembiayaan gelap (*illicit financing*).[65] Pada aspek ini, kripto rentan untuk digunakan sebagai medium yang memfasilitasinya, sebab transaksi menggunakan kripto dapat dilakukan dengan jangkauan lintas negara yang luas.

Meski belum ditemukan kasus spesifik, namun potensi penyalahgunaannya kripto sebagai medium pencucian uang hasil kejahatan lingkungan tetap perlu diwaspadai. Argumentasi ini juga didukung oleh temuan dari Asia Pasific Group-UNODC yang menyebutkan bahwa informasi terkait metode pembayaran ataupun cara lain yang digunakan untuk memfasilitasi kejahatan lingkungan sangatlah sedikit. Selain terdapat faktor bahwa laporan mengenai kejahatan lingkungan tidak lengkap dan terfragmentasi, minimnya informasi mengenai hal ini juga menunjukan bahwa penggunaan instrumen yang memungkinkan aspek anonimitas

---

[62] Benjamin Kurylo, "Explainer: What is Environmental Crime?", *Earth.org,* 25 Maret 2024, https://earth.org/explainer-what-is-environmental-crime/.
[63] Amandra Megarani, "Nilai Kejahatan Lingkungan Rp4.074 Triliun", *Forest Digest,* 1 April 2022, https://www.forestdigest.com/detail/1626/kejahatan-lingkungan
[64] Benjamin Kurylo, *loc.cit.*
[65] Amandra Megarani, *loc.cit.*

dan kompleksitas dalam hal pelacakan sangat mungkin digunakan.[66] Artinya, penggunaan kripto juga berpeluang digunakan sebagai medium penyaluran aset hasil kejahatan lingkungan.

Tak hanya sebagai medium transaksi, kripto juga bisa digunakan untuk menyamarkan uang hasil kejahatan lingkungan melalui pendanaan penambangan kripto. Data Europol pada tahun 2022 menunjukan bahwa operasi pencucian uang menggunakan kripto dilaporkan sebagai proporsi tertinggi dibanding penyalahgunaan kripto untuk tindakan ilegal lainnya seperti misalnya penipuan.[67] Dalam konteks ini, keuntungan hasil kejahatan lingkungan dapat dijadikan sebagai sumber pembiayaan penambangan kripto yang menghasilkan koin digital baru. Tidak ada keterkaitan secara langsung antara koin baru ini dengan aktivitas kriminal maupun kejahatan asalnya, sebab proses penambangan kripto sendiri juga merupakan hal yang legal. Setelah itu, koin tersebut dapat dijual kembali menjadi mata uang fiat, sehingga para pelaku akhirnya mendapati hasil akhir berupa aset yang seolah terlihat bersih, padahal bersumber dari tindak pidana berupa kejahatan lingkungan.

Berdasarkan kemungkinan tersebut, maka diperlukan aturan-aturan terkait mata uang digital, khususnya yang dapat mendukung pencegahan dan penindakan kejahatan-kejahatan yang melibatkan mata uang digital. Tidak adanya aturan-aturan tersebut menimbulkan risiko besar terhadap integritas keseluruhan pasar mata uang digital. Penyalahgunaan mata uang digital beserta pasarnya untuk kejahatan tertentu dapat menyebabkan kurangnya kepercayaan pengguna mata uang digital yang secara signifikan dapat menghambat pengembangan pasar aset tersebut. Hal ini berpotensi membuat hilangnya peluang dalam hal layanan digital inovatif dan adanya alternatif instrumen pembayaran atau sumber pendanaan baru.[68]

C. Pengaturan dan Praktik Umum Terkait Pencegahan dan Penindakan Kejahatan yang Melibatkan Mata Uang Digital

Dalam perkembangannya, terdapat beberapa pihak/lembaga yang mengeluarkan standar atau pengaturan penanganan mata uang digital, termasuk dalam hubungannya dengan penegakan hukum atas kejahatan-kejahatan tertentu yang melibatkan mata uang digital seperti pencucian uang dan pendanaan terorisme. Salah satu standar penanganan mata uang digital tersebut yang banyak diikuti secara global adalah standar-standar yang dikeluarkan oleh FATF. Lembaga ini banyak menerbitkan pengaturan terkait penanganan tindak pidana pencucian dan pendanaan terorisme, yang kemudian memberikan konteks kejahatan-

[66] Stefano Sigia, "Environmental Crimes and Money Laundering", *Pideeco,* 22 Juni 2020, https://pideeco.be/articles/environmental-green-crimes-aml-money-laundering/

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

[68] 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 dan 5

kejahatan tersebut dengan mata uang digital. Misalnya, dokumen FATF pada tahun 2014 yang menjabarkan definisi-definisi dari terminologi dalam transaksi mata uang digital dan potensi keterlibatan mata uang digital dalam kejahatan pencucian uang dan pendanaan terorisme.[69]

Secara umum, pengaturan-pengaturan untuk penegakan hukum terkait mata uang digital dalam dokumen-dokumen FATF dapat dibagi menjadi 2 (dua) bagian, yaitu aturan terkait pencegahan dan penindakan kejahatan. Aturan-aturan terkait pencegahan lebih banyak mengatur tentang sistem transaksi dan kewajiban para pihak yang terlibat dalam transaksi mata uang digital agar dapat menghindari pelibatan mata uang digital dalam kejahatan pencucian uang dan pendanaan terorisme. Sedangkan, aturan terkait penindakan lebih banyak berfokus pada kewenangan lembaga penegak hukum dan kewajiban pihak-pihak yang terlibat dalam transaksi mata uang digital apabila terdapat kejahatan yang diduga melibatkan mata uang digital. Adapun penjelasan lebih lanjut mengenai aturan-aturan tersebut adalah sebagai berikut:

1. Pencegahan

Seperti yang disebutkan sebelumnya, FATF telah mengakui bahwa terdapat risiko terjadinya kejahatan pencucian uang dan pendanaan terorisme yang melibatkan mata uang digital dan aktivitas *Virtual Asset Service Provider* (VASP) sebagai pihak penyedia layanan transaksi mata uang digital. Oleh karena itu, FATF menghimbau agar setiap negara perlu mengambil langkah-langkah pencegahan dengan mengidentifikasi, menilai, dan memahami risiko terjadinya kejahatan-kejahatan tersebut dalam transaksi mata uang digital, setidaknya dengan mempertimbangkan jenis layanan, produk, atau transaksi yang terlibat; risiko profil pengguna layanan; faktor geografis; dan jenis mata uang digital yang dipertukarkan. Tidak hanya perlu dilakukan secara langsung oleh negara, negara juga perlu mewajibkan VASP serta entitas wajib lainnya yang terlibat dalam aktivitas atau operasi keuangan atau menyediakan produk layanan mata uang digital untuk mengidentifikasi, menilai, dan mengambil tindakan efektif untuk memitigasi risiko terjadinya pencucian uang dan pendanaan terorisme dalam pelaksanaan layanan mereka.[70]

Secara umum, FATF merumuskan langkah-langkah pencegahan kejahatan yang melibatkan mata uang digital dalam rekomendasinya nomor 15 dan 16 dalam dokumen pencegahan dan penindakan kejahatan pencucian uang dan pendanaan terorisme. FATF juga merumuskan catatan penafsiran untuk masing-masing rekomendasi tersebut agar dapat lebih mudah diterapkan oleh setiap negara. Beberapa pengaturan penting menurut masing-masing rekomendasi dan catatan interpretasi tersebut adalah sebagai berikut:[71]

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

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

[71] Disarikan dari 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), hal. 16-17, 78-85.

a. *Rekomendasi No. 15 dan Catatan Penafsiran (Interpretative Notes) Rekomendasi No. 15*
   - Negara-negara harus mempertimbangkan mata uang digital sebagai "properti", "hasil", "dana", "dana atau aset lainnya", atau "nilai terkait". Oleh karena itu, negara-negara harus menerapkan langkah-langkah yang relevan berdasarkan rekomendasi-rekomendasi FATF terkait pencegahan dan penindakan kejahatan pencucian uang dan pendanaan terorisme terhadap mata uang digital dan VASP;
   - Negara-negara harus mengidentifikasi, menilai, dan memahami risiko pencucian uang, pendanaan teroris, dan pendanaan proliferasi yang muncul dari aktivitas mata uang digital dan operasi layanan VASP. Berdasarkan penilaian tersebut, negara-negara harus menerapkan pendekatan berbasis risiko untuk memastikan bahwa langkah-langkah untuk mencegah atau memitigasi pencucian uang dan pendanaan teroris sepadan dengan risiko yang diidentifikasi;
   - Negara-negara harus memastikan bahwa penyedia layanan mata uang digital atau VASP telah diatur untuk tujuan anti pencucian uang dan pendanaan terorisme dan tunduk pada sistem yang efektif untuk memantau dan memastikan kepatuhan penyedia layanan mata uang digital terhadap langkah-langkah relevan yang disyaratkan dalam rekomendasi-rekomendasi FATF;
   - Negara harus memastikan bahwa VASP, baik perorangan maupun badan hukum, memiliki lisensi atau terdaftar, setidaknya di yurisdiksi tempat pembuatannya. Negara harus mengambil tindakan untuk mengidentifikasi perorangan atau badan hukum yang melakukan aktivitas VASP tanpa izin atau registrasi yang diperlukan dan menerapkan sanksi yang sesuai;
   - Negara-negara harus mewajibkan VASP untuk mengidentifikasi, menilai, dan mengambil tindakan efektif untuk memitigasi risiko pencucian uang, pendanaan terorisme, dan pendanaan proliferasi. VASP harus tunduk pada sistem yang efektif untuk memantau dan memastikan kepatuhan terhadap kebijakan nasional terkait pencegahan pencucian uang dan/atau pendanaan terorisme;
   - Negara-negara harus memastikan bahwa terdapat serangkaian sanksi yang efektif, proporsional, dan memberikan efek pencegahan, baik pidana, perdata atau administratif, yang tersedia untuk menangani VASP yang gagal mematuhi kebijakan anti pencucian uang dan/atau pendanaan terorisme. Sanksi harus diterapkan tidak hanya kepada VASP, tetapi juga kepada orang-orang yang menjalankan VASP tersebut;
   - VASP harus diawasi atau dipantau oleh otoritas yang kompeten, yang melakukan pengawasan atau pemantauan berbasis risiko serta memiliki kewenangan yang memadai untuk mengawasi dan memastikan kepatuhan VASP terhadap persyaratan untuk memerangi pencucian uang dan pendanaan terorisme. Kewenangan dimaksud antara lain melakukan inspeksi, memaksa VASP untuk memberikan informasi tertentu, dan menjatuhkan sanksi, serta kewenangan untuk menarik, membatasi, atau menangguhkan lisensi atau pendaftaran VASP;
   - Negara harus mengatur di dalam hukum nasional tentang kewajiban VASP untuk melakukan *Customer Due Diligence* (CDD) untuk setiap transaksi mata uang digital sebesar USD/EUR 1,000. Menurut Rekomendasi No. 10 FATF, CDD tersebut dilakukan dengan cara-cara sebagai berikut:

- Mengidentifikasi dan memverifikasi identitas pelanggan menggunakan sumber dokumen, data, atau informasi yang dapat dipercaya dan independen;
- Mengidentifikasi pemilik manfaat (*beneficial owner*) dan mengambil tindakan yang wajar untuk memverifikasi identitas pemilik manfaat, sehingga VASP mengetahui siapa pemilik manfaat tersebut. Dalam hal pemilik manfaat adalah badan hukum, VASP perlu untuk memahami struktur kepemilikan dan kendali dari pihak tersebut;
- Memahami dan, jika perlu, memperoleh informasi tentang tujuan dan sifat hubungan bisnis dan transaksi yang dilakukan;
- Melakukan *due diligence* yang berkelanjutan terhadap hubungan bisnis dan pengawasan terhadap transaksi yang dilakukan selama hubungan tersebut untuk memastikan bahwa transaksi yang dilakukan konsisten dengan pengetahuan VASP tentang nasabah, bisnisnya, dan profil risikonya, termasuk sumber dananya.

- Negara-negara harus memastikan bahwa, dalam setiap transaksi mata uang digital, baik VASP asal (*originating*) maupun tujuan, mendapatkan dan menyimpan informasi yang diperlukan dan akurat tentang profil pengirim dan penerima (*beneficiary*) agar dapat menyediakan informasi-informasi tersebut kepada pihak yang berwenang berdasarkan permintaan.
- Negara-negara harus secara cepat, konstruktif, dan efektif menyediakan kerjasama internasional seluas mungkin sehubungan dengan pencucian uang, tindak pidana asal, dan pendanaan terorisme yang berkaitan dengan mata uang digital. Secara khusus, pengawas VASP harus bertukar informasi secara cepat dan konstruktif dengan mitra asing mereka, terlepas dari sifat atau status pengawas dan perbedaan dalam nomenklatur atau status VASP;
- Ketentuan-ketentuan dalam Rekomendasi No. 16, seperti pengawasan ketersediaan informasi, pelaksanaan tindakan pembekuan (*freezing*), dan pelarangan transaksi terhadap orang atau badan hukum, berlaku pula untuk mata uang digital.

b. *Rekomendasi No. 16 dan Catatan Penafsiran (Interpretative Notes) Rekomendasi No. 16*
   - Rekomendasi ini dikenal pula dengan nama "*Travel Rule*", termasuk untuk transaksi mata uang digital;
   - Negara-negara harus memastikan bahwa lembaga-lembaga keuangan menyertakan informasi yang diperlukan dan akurat mengenai pihak yang memulai transaksi, pihak penerima (*beneficiary*), dan mengenai transaksi *wire transfer* dan pesan-pesan terkait yang dilakukan, serta memastikan bahwa informasi tersebut tetap ada dalam *wire transfer* atau pesan terkait di seluruh rantai pembayaran;
   - Negara-negara harus memastikan bahwa lembaga-lembaga keuangan memantau transaksi *wire transfer* untuk tujuan mendeteksi transaksi yang tidak memiliki informasi mengenai pengirim dan/atau penerima dan mengambil tindakan yang tepat, seperti tindakan pembekuan dan melarang transaksi oleh atau dengan entitas tertentu;
   - *Travel Rule* adalah langkah utama dalam rezim anti pencucian uang/pendanaan terorisme yang memungkinkan VASP dan lembaga keuangan mencegah pelaku

kejahatan terorisme, pencuci uang, dan kejahatan lainnya dengan mengakses *wire transfer* untuk memindahkan dana mereka, termasuk mata uang digital, dan mendeteksi apabila penyalahgunaan tersebut terjadi. Secara khusus, aturan-aturan dalam *Travel Rule* ditujukan untuk memastikan bahwa informasi dasar mengenai pengirim dan penerima dalam transaksi mata uang digital tersedia untuk:

- otoritas penegak hukum guna dapat mendeteksi, menyelidiki dan mengadili para pelaku kejahatan, serta melacak aset mereka;
- unit intelijen keuangan untuk menganalisis aktivitas mencurigakan atau tidak biasa;
- VASP dan lembaga keuangan yang mengirimkan, menjadi perantara, dan menerima transaksi untuk mengidentifikasi dan melaporkan transaksi mencurigakan, serta membekukan dana dan mencegah transaksi oleh atau dengan entitas tertentu.[72]

Selain mengeluarkan rekomendasi-rekomendasi di atas, FATF juga mengeluarkan panduan khusus yang mempermudah pihak-pihak yang terlibat dalam transaksi mata uang digital dalam mencegah terjadinya kejahatan yang melibatkan mata uang digital. Panduan ini berisi indikator-indikator *red flag* tertentu untuk mengkategorikan sebuah transaksi mata uang digital sebagai transaksi yang diduga suatu pencucian uang atau pendanaan terorisme.[73] Bahkan, FATF kemudian menerbitkan panduan terkait tindakan-tindakan yang perlu dilakukan masing-masing pihak di atas, yaitu pihak dalam sektor publik (seperti pengawas transaksi keuangan, penegak hukum, dll)[74], sektor keuangan dan non-keuangan[75], dan VASP[76], dalam dokumen yang terpisah-pisah sesuai dengan peran pihak-pihak tersebut.

2. Penindakan

Secara prinsip, penindakan terhadap mata uang digital tidak perlu menunggu adanya suatu kejahatan. Seperti yang disebutkan sebelumnya, Rekomendasi No. 15 dan 16 FATF telah memungkinkan VASP untuk melakukan pembekuan (*freezing*) apabila terdapat transaksi yang mencurigakan berdasarkan *red flag indicators* atau melanggar ketentuan *Travel Rule*.[77] Ketentuan serupa juga diadopsi oleh Uni Eropa dalam hal sebuah transaksi melanggar peraturan terkait pasar mata uang digital[78] dan Amerika Serikat apabila

[72] Lihat juga 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), hal. 16.

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

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

[75] Lihat 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).

[76] Lihat The Financial Action Task Force (FATF), *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing: Virtual Asset Service Providers,* (Paris: FATF, 2020).

[77] Lihat juga FATF, *Targeted Update on Implementation of the FATF Standard…, Op. Cit.,* hal. 21.

[78] The European Parliament and the Council of the European Union, *markets in crypto-assets…, Op. Cit.,* Art. 94 par. 1.

terdapat transaksi mata uang digital minimal US$500,000, yang dikenal dengan "*administrative forfeiture*"[79].

Namun demikian, ketentuan dan mekanisme penindakan mata uang digital yang terkait dengan kejahatan tetap perlu diatur mengingat adanya potensi sebuah transaksi mata uang digital dalam sebuah kejahatan yang tidak memenuhi *red flag indicators* sehingga tidak mencurigakan atau masih sejalan dengan *Travel Rule*. Dalam konteks ini, diperlukan suatu mekanisme yang dapat mengamankan atau mengambil alih mata uang digital dalam kejahatan tersebut agar nantinya dapat dirampas sebagai hasil kejahatan atau digunakan untuk memulihkan kerugian korban yang terdampak dari kejahatan tersebut. Secara konsep, mekanisme tersebut adalah penyitaan (*seizure*) atau pembekuan (*freezing*) serta perampasan (*confiscation*) mata uang digital yang terindikasi berhubungan dengan suatu kejahatan, yang bertujuan untuk memutus akses pemilik dengan mata uang digital guna mencegah pengalihan, pemindahan, penjualan, atau tindakan lain untuk menghilangkan atau menyamarkan kepemilikan mata uang digital tersebut. Untuk itu, penjabaran bagian ini akan berfokus pada tindakan penindakan berupa penyitaan, pembekuan, atau perampasan mata uang digital yang terindikasi berhubungan dengan suatu kejahatan.

Pada dasarnya, FATF telah mengatur mekanisme penyitaan, pembekuan, dan perampasan mata uang digital tersebut dalam *Guidance on Financial Investigations Involving Virtual Assets* pada tahun 2019. Namun, dikarenakan panduan tersebut bersifat rahasia dan hanya dapat diakses oleh negara-negara anggota FATF[80], ketentuan-ketentuan terkait penyitaan, pembekuan, dan perampasan mata uang digital menurut FATF tidak dapat dijabarkan dalam dokumen ini. Meskipun begitu, negara-negara anggota FATF di kawasan amerika latin, yang bergabung dalam wadah bernama GAFILAT, kemudian menerbitkan panduan investigasi, identifikasi, penyitaan, dan perampasan mata uang digital pada tahun 2021, yang juga banyak merujuk pada dokumen tertutup milik FATF. Beberapa ketentuan penyitaan dan perampasan mata uang digital menurut panduan GAFILAT tersebut adalah sebagai berikut:[81]

(1) Terdapat beberapa prinsip umum yang berlaku dalam penyitaan/pembekuan mata uang digital, seperti:
   - Penyitaan atau pembekuan mata uang digital sama dengan penyitaan barang lainnya, yaitu harus dilakukan berdasarkan izin atau perintah pengadilan. Oleh karena itu, setiap pihak yang ingin melakukan penyitaan/pembekuan terhadap mata uang digital harus mengajukan izin atau mendapatkan perintah dari pengadilan terlebih dahulu sebelum penyitaan/pembekuan dilakukan. Hanya saja, pihak yang menerima perintah dan mekanisme penyitaan/pembekuan

[79] U.S. Department of Justice: Criminal Division, *Asset Forfeiture Policy Manual 2023,* (Washington: U.S. Department of Justice, 2023), hal. 5.2.

[80] 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), hal. 15.

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

tersebut sangat bergantung pada hal-hal terkait mata uang digital yang hendak disita/dibekukan, yang perlu ditentukan sebelum penyitaan/pembekuan dilakukan;

- Karena tingkat kesulitan teknisnya yang lebih besar dibandingkan dengan penyitaan aset biasa dan dibutuhkan kecepatan untuk menjamin keberhasilan penyitaan, tindakan penyitaan atau pembekuan mata uang digital sebaiknya dilakukan oleh personel yang memiliki keahlian dan terlatih. Oleh karena itu, pihak yang melakukan tindakan tersebut perlu menyadari berbagai jenis *wallet* mata uang digital beserta mekanisme keamanannya;
- Seluruh mata uang digital yang telah disita harus ditransfer ke *wallet* milik atau yang dikelola oleh negara/pemerintah. Hal ini penting dilakukan untuk mencegah pelaku atau pihak lain mengambil atau mengalihkan mata uang digital tersebut sebelum proses hukum selesai dilakukan. Untuk itu, penting bagi penegak hukum mengetahui jenis mata uang digital yang akan disita dan negara perlu untuk memiliki *wallet* khusus untuk setiap mata uang digital mengingat mata uang digital hanya dapat ditransfer ke alamat yang sesuai dengan *blockchain* mereka sendiri. Misalnya, Bitcoin hanya dapat dikirim ke alamat Bitcoin, Monero ke alamat Monero, dll;

(2) Secara umum, penyitaan/pembekuan mata uang digital dilakukan dalam 3 (tiga) tahap, yaitu: (i) perencanaan penyitaan; (ii) pelaksanaan penyitaan; dan (iii) pengelolaan aset pasca penyitaan;

(3) Pada tahap perencanaan penyitaan, beberapa hal yang perlu dilakukan antara lain:

a) Mengetahui jenis mata uang digital yang akan disita/dibekukan beserta sistem transaksi dan metode penyimpanannya. Hal pertama yang perlu diketahui adalah apakah mata uang digital tersebut ditransaksikan secara terpusat/*centralized* oleh suatu otoritas administratif pusat, yaitu perusahaan atau entitas yang mengembangkan dan mengoperasikan mata uang, atau terdesentralisasi;

b) Apabila transaksi mata uang digital tersebut dilakukan secara terpusat, maka penegak hukum dapat segera meminta pengadilan untuk menerbitkan izin/perintah pembekuan atau penyitaan mata uang digital kepada otoritas pusat tersebut;

c) Apabila transaksi mata uang digital dilakukan secara terdesentralisasi, maka penegak hukum harus mengidentifikasi apakah mata uang digital yang akan disita disimpan di *wallet* kustodian (*custodial wallet*[82]) dimana *private key* yang diperlukan untuk mentransaksikan mata uang digital disimpan dan berada di bawah tanggung jawab VASP. Tindak lanjut dari hasil identifikasi tersebut adalah:

- Apabila mata uang digital dan *private key* disimpan oleh VASP, maka penegak hukum dapat segera meminta pengadilan untuk menerbitkan perintah

[82] *Custodial wallet* adalah layanan mata uang digital di mana mata uang digital dan/atau sarana akses pengguna (misalnya *private key*) disimpan oleh penyedia layanan atas nama pengguna. Pengguna berinteraksi dengan penyedia layanan, bukan dengan *blockchain*, untuk mengelola mata uang digital miliknya. *Custodian wallet* juga dikenal sebagai "*hosted wallet*". Lihat International Organization of Securities Commissions (IOSCO), *Policy Recommendations for Crypto and Digital Asset Markets: Final Report*, (Madrid, IOSCO, 2023), hal. 45. Lihat juga International Organization of Securities Commissions (IOSCO), *Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms: Final Report,* (Madrid: IOSCO, 2020), hal. 12 – 13.

pembekuan mata uang digital kepada VASP tersebut untuk kemudian ditransfer ke alamat atau *wallet* yang dikuasai negara; atau

- Apabila mata uang digital dan *private key* tidak disimpan dalam *wallet* milik VASP (*non-custodial wallet*[83]), maka penyimpanan dan pengelolaan mata uang digital tersebut dilakukan secara langsung oleh pelaku. Untuk itu, penyitaan harus dilakukan dengan memperoleh informasi mengenai *private key* atau *seed words* yang dapat memberikan akses penegak hukum kepada mata uang digital atau *wallet* untuk kemudian mentransfer mata uang digital tersebut ke *dompet* yang dikuasai negara. Dalam kondisi tersebut, maka permintaan izin penyitaan ke pengadilan harus dilakukan dengan memperhatikan hal-hal sebagai berikut:
  - Jenis *wallet* yang dikuasai pelaku dapat berupa: (i) *wallet* virtual berbentuk *software* yang tersimpan di *desktop* komputer sebagai aplikasi atau *wallet* di telepon seluler, seperti Mycelium, Greenbits, Breadwallet, dan Airbitz; atau (ii) *wallet* perangkat keras yang menyimpan *private key* pada perangkat portable, seperti *pen drive* atau dicetak di kertas;
  - Untuk itu, penegak hukum perlu meminta izin ke pengadilan untuk menyita seluruh perangkat penyimpanan data yang ditemukan saat penggeledahan, seperti komputer, telepon seluler, *hard disk* portabel, CDR, DVDR, *memory stick, flashdisk,* atau barang-barang lain yang berpotensi menyimpan informasi terkait *wallet, private key* atau *seed words* yang dapat memberikan akses penegak hukum kepada mata uang digital;
  - Penegak hukum perlu mempertimbangkan untuk meminta izin pengadilan agar dapat langsung melakukan penyitaan mata uang digital apabila perangkat penyimpan informasi mata uang digital dalam kondisi tidak terkunci dan aktif. Hal ini dikarenakan peluang ideal untuk mendapatkan mata uang digital adalah ketika *wallet* yang berisi *private key* terbuka, atau ketika kata sandi untuk membukanya atau "*seed words*" untuk mengakses *wallet* tersebut ditemukan saat penggeledahan;
  - Penegak hukum juga perlu mempertimbangkan kebutuhan untuk sesegera mungkin menetralisir segala kemungkinan bahwa pemilik mata uang digital menghancurkan, mengubah, atau menyembunyikan informasi yang berguna untuk mengakses *wallet* mata uang digital (kata sandi atau pin tulisan tangan, dompet perangkat keras, dll), mengalihkan mata uang digital, atau memberitahu pihak lain untuk melakukan hal-hal tersebut sebelum penegak hukum berhasil mengakses *wallet* tersebut;
  - Dalam hal penegak hukum telah memperoleh izin pengadilan, maka penegak hukum perlu segera menyiapkan *wallet* yang dikuasai negara untuk menerima transfer mata uang digital yang akan disita sesuai dengan jenis mata uang digital tersebut;

(4) Pada tahap pelaksanaan penyitaan, beberapa hal yang perlu dilakukan antara lain:

[83] *Non-custodial wallet* adalah perangkat lunak atau perangkat keras yang menyimpan kunci kriptografi untuk pengguna, membuat mata uang digital pengguna hanya dapat diakses oleh pengguna, dan memungkinkan pengguna untuk berinteraksi langsung dengan blockchain dan aplikasi keuangan berbasis blockchain. *Non-custodial wallet* juga dikenal sebagai "*unhosted wallet*". Liat *Ibid.*

a) Melakukan penyitaan terhadap mata uang digital sesuai dengan jenis mata uang digital atau *wallet* penyimpan mata uang digital tersebut (yang dijabarkan secara rinci untuk setiap jenis mata uang digital dan *wallet* dalam panduan oleh GAFILAT) dan mentransfer mata uang digital yang disita ke *wallet* yang dikuasai negara;
b) Penegak hukum perlu mempertimbangkan untuk mengisolasi pemilik mata uang digital dan semua orang lain yang hadir selama proses penyitaan berlangsung untuk mencegah mereka terhubung ke Internet atau melakukan kontak dengan dunia luar hingga penyitaan selesai;
c) Apabila penegak hukum menemukan perangkat yang menyimpan *wallet*, namun *wallet* tersebut diblokir dan penegak hukum tidak menemukan kata sandi yang diperlukan untuk mengaksesnya, maka penegak hukum menyita perangkat yang berisi *wallet* tersebut dengan tindakan-tindakan seperti pada penanganan bukti elektronik. Selanjutnya, tindakan investigasi yang relevan harus dilakukan sesegera mungkin untuk mendapatkan kata sandi dan menyita mata uang digital;
d) Apabila akses ke *wallet* tersebut tidak dapat diperoleh atau *wallet* ditemukan kosong setelah dibuka, penegak hukum dapat mengidentifikasi nilai dari mata uang digital yang akan disita melalui *blockchain* dan melakukan penyitaan aset lain yang nilainya setara dengan mata uang digital tersebut;
e) Apabila *wallet* ditemukan dalam keadaan tidak diblokir, maka penyitaan dapat langsung dilakukan berdasarkan izin pengadilan dan mentransfer mata uang digital yang disita ke *wallet* yang dikuasai negara;

(5) Pada tahap pasca penyitaan, beberapa hal yang perlu dilakukan antara lain:
a) Secara garis besar, terdapat 2 (dua) alternatif yang dapat dilakukan terhadap mata uang digital yang disita, yaitu:
- **Tetap menyimpan mata uang digital dalam bentuk yang sama ketika penyitaan dilakukan sampai putusan dijatuhkan**. Keuntungan dari alternatif ini adalah mata uang digital hanya dijual setelah putusan akhir, sehingga apabila pelaku diputus bebas, maka mata uang digital tersebut dapat langsung dikembalikan. Kerugiannya terletak pada risiko yang melekat pada keamanan pemeliharaan mata uang digital dan biaya-biaya lain yang terkait dengannya;
- **Mengkonversi mata uang digital ke dalam mata uang fiat sesegera mungkin**. Keuntungan dari alternatif ini terletak pada pengurangan risiko keamanan yang terkait dengan pemeliharaan mata uang digital dan biaya yang terkait dengannya. Kerugiannya terletak pada kemungkinan perbedaan nilai mata uang digital tersebut ketika dikonversi ke mata uang fiat dan saat putusan akhir, khususnya ketika mata uang digital tersebut harus dikembalikan kepada pelaku karena pengadilan memutuskan pelaku tidak bersalah;

b) Alternatif lain adalah menetapkan terlebih dahulu melalui peraturan atau kebijakan internal terkait jangka waktu tetap untuk melakukan konversi mata uang digital yang disita menjadi mata uang fiat (misalnya, tiga hari). Dengan begitu, keputusan untuk melakukan konversi tersebut tidak bergantung pada penilaian tentang keuntungan dalam hal ekonomi, melainkan berdasarkan aturan tertulis dari negara;

c) Apabila mata uang digital diputuskan untuk disimpan dalam bentuk yang sama, maka penegak hukum melakukan hal-hal sebagai berikut:
   - Menyimpan mata uang digital dalam *cold wallet*, seperti *wallet* perangkat keras, *wallet* virtual dalam perangkat yang tidak terhubung dengan internet, atau dalam *wallet* kertas;
   - Menyimpan kata sandi, *private key*, *seed words*, pin, dan alamat mata uang digital dalam file teks pada folder khusus untuk setiap mata uang digital yang disita pada perangkat penyimpanan eksternal, seperti *hard drive* portabel, yang kemudian dienkripsi. Perangkat ini harus tetap *offline* di lokasi aman tertentu sampai diperlukan oleh penegak hukum;
   - Menunjuk pejabat tertentu untuk menyimpan perangkat yang berisi informasi kata sandi, *private key*, *seed words*, pin, dan alamat mata uang digital dan membatasi akses ke perangkat tersebut;
   - Apabila penegak hukum tidak memiliki struktur keamanan siber yang dapat diandalkan untuk penyimpanan mata uang digital, penegak hukum dapat menunjuk suatu VASP dapat dipercaya untuk mengelola mata uang digital;
d) Apabila mata uang digital diputuskan untuk dikonversi ke mata uang fiat, maka penegak hukum melakukan penjualan terhadap mata uang digital tersebut, baik secara langsung, maupun melalui lelang umum, dengan selalu mengupayakan nilai maksimal dari penjualan tersebut. Konversi tersebut juga dapat dilakukan dengan kesepakatan dengan VASP yang memiliki spesialisasi dalam pertukaran mata uang digital untuk melakukan konversi mata uang digital tersebut menjadi mata uang fiat;
e) Beberapa praktik di negara-negara tertentu terkait tindakan atas mata uang digital yang telah disita adalah:
   - Di Belanda, keputusan terkait tindakan atas mata uang digital diambil berdasarkan pendapat tertulis dari pemilik mata uang digital, apakah ia lebih memilih mata uang digital tersebut disimpan dalam keadaan aslinya atau dikonversi menjadi mata uang fiat. Dengan cara ini, apabila mata uang digital tersebut harus dikembalikan di kemudian hari, Negara dibebaskan dari tanggung jawab atas hilangnya nilai akibat fluktuasi harga mata uang digital yang bersangkutan;
   - Di Amerika Serikat, mata uang digital diputuskan untuk tidak dikonversi ke dalam mata uang fiat dan tetap menyimpannya sesuai dengan bentuk aslinya dengan kemudian menerapkan langkah-langkah keamanan yang diperlukan untuk memastikan penyimpanan yang efektif atas mata uang digital tersebut.

Secara umum, ketentuan-ketentuan di atas juga diatur serupa dalam standar atau panduan terkait penyitaan, pembekuan, dan perampasan mata uang digital yang dikeluarkan oleh pihak lain. Beberapa di antaranya adalah panduan yang diterbitkan oleh StAR (*the Stolen Asset Recovery Initiative*) yang merupakan kerja sama antara *World Bank Group* dan *the United Nations Office on Drugs and Crime* (UNODC)[84] dan Uni Eropa

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

melalui *Cybercrime Programme Office of the Council of Europe* (C-PROC)[85]. Ketentuan serupa juga dapat ditemukan dalam hukum domestik dan praktik di beberapa negara, seperti negara-negara Britania Raya (*United Kingdom*) yang melaksanakan penyitaan, pembekuan, dan perampasan aset mata uang digital berdasarkan *Proceeds of Crime Act 2002* (POCA)[86], Amerika Serikat yang mengacu pada aturan umum penyitaan dalam *Rules 41 Federal Rules of Criminal Procedure* dan melaksanakan secara teknis dengan mengacu pada *Asset Forfeiture Policy Manual 2023* yang diterbitkan oleh *U.S. Department of Justice*[87], dan Malaysia yang secara teknis melakukan hal-hal tersebut menurut panduan yang diterbitkan oleh *National Anti-Financial Crime Center* (NFCC) and *CyberSecurity Malaysia* (CSM)[88].

Secara umum, aturan-aturan pencegahan dan penindakan kejahatan pencucian uang dan pendanaan terorisme, termasuk yang melibatkan mata uang digital, perlu untuk diterapkan dengan benar oleh entitas-entitas yang diwajibkan untuk itu. Dalam hal ini, diperlukan suatu kerja sama dan peran yang kuat dari lembaga-lembaga di bawah negara yang terkait dengan pencegahan dan pencucian uang sebagai otoritas yang kompeten dalam menegakkan aturan-aturan tersebut. Uni Eropa mencontohkan kerja sama antar lembaga ini yang perlu melibatkan banyak *stakeholders*, seperti FIU, penegak hukum yang memiliki fungsi penyidikan dan penuntutan kejahatan pencucian uang, tindak pidana asal terkait, dan pendanaan terorisme, otoritas dengan fungsi penelusuran, penyitaan, dan pembekuan aset-aset pelaku kejahatan, pihak yang berwenang untuk menerima laporan terkait transaksi mata uang (termasuk mata uang digital) lintas batas negara, serta pihak berwenang yang bertanggung jawab melakukan pengawasan atau pemantauan guna memastikan kepatuhan entitas-entitas tertentu terhadap aturan-aturan pencegahan dan penindakan pencucian uang.[89]

Dalam praktiknya, Amerika Serikat adalah salah satu negara yang telah menerapkan kerja sama antar lembaga pemerintah dan penegak hukum dalam melakukan pencegahan dan

---

[85] The European Parliament and the Council of the European Union, *markets in crypto-assets…, Op. Cit.,* Art. 94 par. 3. Untuk aturan teknis penyitaan, pembekuan, dan perampasan mata uang digital, lihat Cybercrime Programme Office of the Council of Europe (C-PROC), *Guide On Seizing Cryptocurrencies,* (Bucharest: C-PROC, 2021), hal. 19 – 118.

[86] Lihat United Kingdom, *Proceeds of Crime Act 2002* (POCA), Pasal 47C ayat (5A) – (5F), Pasal 47M ayat (2A) dan (2B), Pasal 47R ayat (6), Pasal 67ZA, Pasal 67ZB, Pasal 67AA, Pasal 127C ayat (5A) – (5F), Pasal 127M ayat (2A) dan (2B), Pasal 127Q ayat (6), Pasal 131ZB, Pasal 131ZC, Pasal 131AA, Pasal 195C ayat (5A) – (5F), Pasal 195M ayat (2A) dan (2B), Pasal 195R ayat (6), Pasal 215ZA, Pasal 215ZB, Pasal 215AA, dan Chapter 3C – 3F. Lihat juga Skadden, "*Cryptoasset Seizures and Forfeitures…, Loc. Cit.*

[87] U.S. Department of Justice: Criminal Division, *Asset Forfeiture Policy Manual 2023…, Op. Cit.,* hal. 2.10 – 2.12. Lihat juga aturan teknis internal kepolisian lokal di beberapa negara bagian Amerika Serikat, seperti Indiana (Indiana State Police, "*Standard Operating Procedure: Seizure of Cryptocurrency and Virtual Currencies*", https://www.in.gov/isp/files/Seizure-of-Cryptocurrency.pdf , diakses pada Jum'at, 16 Februari 2024) dan 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 , diakses pada Jum'at, 16 Februari 2024).

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

[89] The European Parliament and the Council of the European Union, *Amending Directive (EU) 2015/849…, Op. Cit.,* par. 44.

penindakan kejahatan yang melibatkan mata uang digital. Hal ini seperti yang disampaikan oleh Jaksa Agung (*Attorney General*) Amerika Serikat, Merrick B. Garland, sebagai alasan pembentukan *Digital Asset Coordinator* (DAC) *Network* pada tanggal 16 September 2022 dimana kerja sama antar departemen dan lembaga di seluruh pemerintahan diperlukan untuk mencegah dan menghentikan eksploitasi mata uang digital untuk memfasilitasi kejahatan seiring dengan semakin meningkatnya peran mata uang digital dalam sistem keuangan global. Asisten Jaksa Agung, Kenneth A. Polite Jr., kemudian menambahkan bahwa perkembangan mata uang digital telah menciptakan lanskap baru untuk mengeksploitasi inovasi tersebut oleh para pelaku kejahatan dan DAC dibentuk agar *Department of Justice* Amerika Serikat dan Jaksa-jaksanya berada pada posisi terbaik untuk memerangi kejahatan yang melibatkan mata uang digital.[90]

Pada dasarnya, DAC *Network* bukanlah wadah kerja sama antar lembaga atau aksi pertama dalam pencegahan dan penindakan kejahatan yang melibatkan mata uang digital di Amerika Serikat. Terdapat beberapa unit atau aksi lain sebelum DAC *Network* dibentuk, antara lain:[91]

1. Pada tahun 2018, *Money Laundering and Asset Recovery Section* (MLARS) di bawah Divisi Kriminal *Department of Justice* Amerika Serikat meluncurkan "*the Digital Currency Initiative*" yang berfokus memberikan dukungan dan bimbingan kepada penyidik, jaksa, dan lembaga pemerintah lainnya mengenai penuntutan dan penyitaan mata uang digital;
2. Pada tahun 2020, *the Cyber-Digital Task Force* di bawah Jaksa Agung meluncurkan "*the Cryptocurrency Enforcement Framework*" yang menjelaskan perangkat hukum yang tersedia untuk melakukan penuntutan atas penggunaan mata uang digital secara illegal, membuat profil peran dan tanggung jawab setiap departemen dan lembaga pemerintah di bidang aset/mata uang digital, serta mencatat strategi untuk mengatasi ancaman yang muncul terhadap keamanan dan pengoperasian pasar mata uang digital yang efektif;
3. Pada tahun 2021, *Department of Justice* Amerika Serikat mengumumkan pembentukan *National Cryptocurrency Enforcement Team* (NCET) yang beranggotakan jaksa federal, penyidik, dan staf pendukung lainnya seperti ahli dari MLARS, kantor kejaksaan, FBI, dan *financial regulator*. NCET memiliki tugas prioritas untuk menyusun strategi terkait teknologi mata uang digital, mengidentifikasi area-area peningkatan fokus investigasi dan penuntutan, menangani masalah yang timbul dari penerapan aturan yang ada terhadap penggunaan mata uang digital, dan memimpin upaya Departemen untuk berkoordinasi dengan mitra penegakan hukum domestik dan internasional, badan pembentuk aturan, dan industri swasta untuk memerangi kejahatan yang melibatkan mata uang digital;

---

[90] U.S. Department of Justice, *Justice Department Announces Report on Digital Assets and Launches Nationwide Network,* Rilis Pers, Jum'at, 16 September 2022. Dapat diakses di https://www.justice.gov/opa/pr/justice-department-announces-report-digital-assets-and-launches-nationwide-network . DAC sendiri dipimpin oleh *National Cryptocurrency Enforcement Team* (NCET), sebuah unit di bawah *Department of Justice* Amerika Serikat, dengan jaringan yang terdiri dari lebih dari 150 orang Jaksa federal yang ditunjuk oleh *U.S. Attorneys' Offices* dan seluruh komponen litigasi di departemen tersebut, dan akan berfungsi sebagai forum utama di departemen tersebut bagi para jaksa untuk memperoleh dan menyebarkan pelatihan khusus, keahlian teknis, dan panduan tentang penyelidikan dan penuntutan kejahatan yang melibatkan mata uang digital.

[91] 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), hal. 14 – 16.

4. Pada Februari 2022, FBI membentuk *the Virtual Asset Exploitation Unit* (VAXU), yaitu sebuah tim khusus untuk melakukan investigasi terhadap kejahatan yang melibatkan mata uang digital. VAXU dibentuk untuk menyatukan para ahli mata uang digital ke dalam suatu unit guna dapat menyediakan peralatan dan teknologi yang dibutuhkan, analisis *blockchain*, pelatihan penyitaan mata uang digital, serta pelatihan terkait mata uang digital lainnya untuk personel FBI. Unit yang bekerja dekat dengan NCET ini juga beranggotakan jaksa dengan keahlian terkait pencucian uang, kejahatan komputer, penyitaan, dan pembentukan kebijakan/peraturan untuk mengejar mereka yang menyalahgunakan mata uang digital untuk melakukan kejahatan[92].

B. Pengaturan dan Praktik Terkait Pencegahan dan Penindakan Kejahatan Yang Melibatkan Mata Uang Digital di Indonesia

Saat ini, transaksi mata uang digital menjadi salah satu pilihan aktivitas keuangan di Indonesia. Menurut Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti), transaksi mata uang digital pada tahun 2021 tercatat sebesar Rp859,4 triliun, Rp306,4 triliun pada tahun 2022, dan Rp149,25 triliun di tahun 2023, serta diharapkan tumbuh kembali di tahun 2024. Tidak hanya itu, hingga saat ini tercatat 501 mata uang digital yang resmi terdaftar dan terdapat 33 Pedagang Fisik Aset Kripto (mata uang digital) yang terdaftar dan teregulasi di Bappebti.[93]

Pengakuan mata uang digital di Indonesia pertama kali diatur dalam Peraturan Menteri Perdagangan No. 99 Tahun 2018 tentang Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto (*Crypto Asset*). Aturan ini dibentuk sebagai respon berkembang luasnya aset kripto/mata uang digital di masyarakat serta bertujuan untuk melindungi masyarakat dan memberikan kepastian hukum kepada pelaku usaha di bidang Perdagangan Berjangka[94]. Dalam aturan ini, aset kripto ditetapkan sebagai komoditi yang dapat diperdagangkan di Bursa Berjangka, yang pembinaan, pengawasan, dan pengembangannya ditetapkan oleh Kepala Bappebti[95]. Untuk melaksanakan aturan ini, Bappebti menerbitkan 2 (dua) aturan teknis, yaitu:

1. Peraturan Bappebti No. 5 Tahun 2019 *jo.* Peraturan Bappebti No. 3 Tahun 2020 yang pada intinya mengatur aturan-aturan teknis perdagangan aset kripto di bursa berjangka.[96] Aturan ini kemudian diperbarui dengan Peraturan Bappebti No. 8 Tahun 2021 *jo.* Peraturan Bappebti No. 13 Tahun 2022[97];

---

[92] Disampaikan oleh *Deputy Attorney General* Amerika Serikat, Lisa O. Monaco, dalam sambutannya pada *The Annual Munich Cyber Security Conference*, Washington D.C., Kamis, 17 Februari 2022. Teks lengkap dapat diakses di https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security

[93] 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 , diakses pada Jum'at, 1 Maret 2024.

[94] Peraturan Menteri Perdagangan Republik Indonesia No. 99 Tahun 2018 Tentang Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto (*Crypto Asset*), bagian "Menimbang" huruf b dan c.

[95] *Ibid.,* Pasal 1 dan 2.

[96] Lihat Peraturan Bappebti No. 5 Tahun 2019 *jo.* Peraturan Bappebti No. 3 Tahun 2020 tentang Ketentuan Teknis Penyelenggaraan Pasar Fisik Aset Kripto (*Crypto Asset*) di Bursa Berjangka.

[97] Lihat Peraturan Bappebti No. 8 Tahun 2021 *jo.* Peraturan Bappebti No. 13 Tahun 2022 Tentang Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (*Crypto Asset*) di Bursa Berjangka

2. Peraturan Bappebti No. 7 Tahun 2020 yang pertama kali menetapkan 229 mata uang digital yang terdaftar dan dapat diperdagangkan di Indonesia[98]. Bappebti kemudian memperbarui aturan ini dengan menambahkan jumlah mata uang digital yang terdaftar dan dapat diperdagangkan di Indonesia menjadi 510 jenis mata uang melalui Peraturan Bappebti No. 11 Tahun 2022 *jo.* Peraturan Bappebti No. 4 Tahun 2023[99].

Secara umum, aturan-aturan di atas sudah mengakomodir ketentuan-ketentuan pencegahan pelibatan mata uang digital dalam kejahatan seperti dalam Rekomendasi dan Catatan Penafsiran Rekomendasi FATF No. 15 dan 16. Misalnya, syarat dan mekanisme mata uang digital/kripto agar dapat diperdagangkan di Indonesia[100], syarat dan mekanisme penetapan serta kewajiban Bursa Berjangka[101], Pedagang Fisik Aset Kripto[102], dan Pengelola Tempat Penyimpan Aset Kripto[103] agar dapat beroperasi di Indonesia, kewajiban Pedagang Fisik Aset Kripto untuk menerapkan prinsip *Know Your Customer* (KYC) dan *Customer Due Diligence* (CDD)[104] serta *Know Your Transaction* (KYT)[105] dan hak Pedagang Fisik Aset Kripto untuk menolak calon Pelanggan Aset Kripto berdasarkan hasil KYC dan CDD[106], syarat dan mekanisme perdagangan aset kripto[107], mulai dari pembukaan rekening, penempatan dana dan aset kripto, transaksi kripto, hingga penarikan aset kripto, lembaga pengawas perdagangan kripto[108], dll. Selain itu, aturan-aturan di atas juga sudah mengatur sanksi-sanksi yang dapat dikenakan kepada pihak-pihak yang melanggar aturan perdagangan aset kripto[109]. Bahkan, aturan-aturan di atas mengatur secara khusus "Penerapan Prinsip *Travel Rules*" yang sejalan dengan Rekomendasi FATF No. 16[110].

Seiring dengan perkembangan transaksi mata uang digital, terdapat pula beberapa kejahatan di Indonesia yang melibatkan mata uang digital. Hal ini diakui oleh Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) yang menyebutkan salah satu modus aliran uang dalam kasus-kasus pencucian uang, khususnya terkait investasi bodong atau

---

[98] Lihat Peraturan Bappebti No. 7 Tahun 2020 tentang Penetapan Daftar Aset Kripto Yang Dapat Diperdagangkan di Pasar Fisik Aset Kripto.

[99] Peraturan Bappebti No. 11 Tahun 2022 *jo.* Peraturan Bappebti No. 4 Tahun 2023 Tentang Penetapan Daftar Aset Kripto yang Diperdagangkan di Pasar Fisik Aset Kripto.

[100] Peraturan Bappebti No. 8 Tahun 2021 *jo.* Peraturan Bappebti No. 13 Tahun 2022…, *Op. Cit.,* Pasal 3.

[101] *Ibid.,* Pasal 5 – 8.

[102] *Ibid.,* Pasal 13 – 16 dan 40 – 42. Lihat juga Peraturan Bappebti No. 11 Tahun 2022 *jo.* Peraturan Bappebti No. 4 Tahun 2023…, *Op. Cit.,* Pasal 1 dan 8.

[103] *Ibid.,* Pasal 17 – 22.

[104] *Ibid.,* Pasal 26 – 28 dan Pasal 32 ayat (3) dan (4).

[105] *Ibid.,* Pasal 39.

[106] *Ibid.,* Pasal 16 ayat (3) huruf a.

[107] *Ibid.,* Pasal 25 – 37.

[108] Pada awalnya, pengawasan perdagangan mata uang digital/kripto merupakan kewenangan Bappebti. Lihat *Ibid.,* Pasal 1 angka 1. Namun, dalam perkembangannya, kewenangan pengawasn tersebut beralih ke Otoritas Jasa Keuangan (OJK). Lihat Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan *jo.* UU No. 4 tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan, Pasal 6 ayat (1) huruf e.

[109] *Ibid.,* Pasal 47 – 49. Lihat juga Peraturan Bappebti No. 11 Tahun 2022 *jo.* Peraturan Bappebti No. 4 Tahun 2023…, *Op. Cit.,* Pasal 9.

[110] Peraturan Bappebti No. 8 Tahun 2021 *jo.* Peraturan Bappebti No. 13 Tahun 2022…, *Ibid.,* Pasal 38.

ilegal, adalah disimpan dalam bentuk mata uang digital/kripto.[111] Faktanya, telah terdapat beberapa kasus yang melibatkan mata uang digital, seperti kasus korupsi PT Asabri (Persero) yang diduga melibatkan tindakan pencucian uang melalui Bitcoin[112], kasus Indra Kesuma alias Indra Kenz yang melakukan tindak pidana penipuan dan memiliki aset kripto yang disita senilai Rp35 miliar[113], dan kasus Donny Alven yang melakukan peretasan akun kripto dari tahun 2017 hingga 2024 dengan total aset yang disita senilai Rp5,1 miliar[114].

Namun, aparat penegak hukum masih kesulitan dalam menangani aset kripto atau mata uang digital yang berkaitan dengan tindak pidana. Setidaknya, terdapat 2 (dua) hal yang menyebabkan sulitnya aparat penegak hukum dalam menangani aset kripto, yaitu minimnya pengaturan terkait aset kripto, khususnya terkait penyitaan aset kripto, dan pengalaman serta pengetahuan aparat penegak hukum tentang aset kripto dan penanganannya[115]. Dalam praktiknya, hambatan tersebut dapat terlihat dari gagalnya aparat penegak hukum melakukan penyitaan terhadap Bitcoin milik Heru Hidayat dan Benny Tjokrosaputro di Pedagang Fisik Aset Kripto bernama Indodax, yang diduga merupakan media penyimpanan hasil korupsi PT ASABRI, karena akun Bitcoin sudah dalam keadaan kosong ketika penyitaan hendak dilakukan[116]. Belum lagi, terdapat pula potensi hambatan seperti yang dialami kejaksaan di Kota Kempten, Jerman, yang berhasil melakukan penyitaan terhadap *wallet* Bitcoin berisi 1.700 BTC senilai lebih dari £50 juta (sekitar Rp841 miliar), namun tidak berhasil membuka *wallet* tersebut karena pemiliknya menolak memberikan *password* dari *wallet* tersebut[117]. Untuk itu, diperlukan suatu aturan yang komprehensif mengenai penanganan, khususnya penyitaan, mata uang digital/aset kripto yang berkaitan dengan tindak pidana di Indonesia.

Sejauh ini, ketentuan penanganan mata uang digital yang berkaitan dengan tindak pidana baru diatur pada tahun 2023 oleh Kejaksaan melalui Pedoman Jaksa Agung No. 7 Tahun 2023 tentang Penanganan Aset Kripto Sebagai Barang Bukti Dalam Perkara Pidana, yang pada intinya mengatur hal-hal antara lain:

---

[111] "Optimalisasi Pengembalian Aset & Keuangan Negara: PPATK Perkuat Analisis & Pemeriksaan Transaksi Keuangan", PPATK, 15 April 2022, https://www.ppatk.go.id/siaran_pers/read/1188/optimalisasi-pengembalian-aset-keuangan-negara-ppatk-perkuat-analisis-pemeriksaan-transaksi-keuangan.html.

[112] Novina Putri Bestari, "Saat Cuci Uang di Bitcoin Jadi Modus Baru Korupsi Asabri", *CNBC Indonesia*, 21 April 2021, https://www.cnbcindonesia.com/tech/20210420232119-37-239412/saat-cuci-uang-di-bitcoin-jadi-modus-baru-korupsi-asabri.

[113] 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.

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

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

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

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

(1) Permohonan persetujuan atau izin penyitaan mata uang digital/aset kripto diajukan ke Ketua Pengadilan Negeri sesuai dengan aturan penyitaan dalam KUHAP. Dalam hal aset kripto berada di luar negeri, maka permohonan persetujuan atau izin penyitaan tersebut diajukan ke Ketua Pengadilan Negeri Jakarta Pusat;[118]
(2) Pemblokiran akun dan *wallet* saat penyitaan aset kripto dilakukan oleh *Digital Evidence First Responder* (DEFR) atas perintah jaksa/penyidik. DEFR adalah pegawai yang berkompeten atau ahli yang diberi tugas melakukan penanganan pertama terhadap aset kripto dengan tanggung jawab menangani aset kripto;[119]
(3) Pemblokiran aset kripto hanya dilakukan terhadap aset kripto yang tersentralisasi (*centralized*) melalui Pedagang Fisik Aset Kripto. Sedangkan, aset kripto yang tidak tersentralisasi (*decentralized*) tidak dapat dilakukan pemblokiran;[120]
(4) Aset kripto yang berhasil disita dapat diamankan dengan dipindahkan oleh DEFR dari *wallet* pemilik ke *Controlled Cryptowallet* yang berbentuk *hardware wallet* dan sesuai dengan jenis aset kripto yang disita. Pemindahan aset kripto ini dilakukan apabila nilai aset kripto tergolong besar dan/atau pertimbangan kemanfaatan penanganan perkara;[121]
(5) *Controlled Cryptowallet* dan *Controlled Address* dibuat oleh pejabat yang menyelenggarakan tata kelola barang bukti dan barang rampasan atas permintaan Jaksa, baik sebelum maupun sesudah penyitaan, dan dibuat sesuai dengan aset kripto yang akan disita. Pejabat tersebut juga berwenang untuk melakukan pengamanan, pengawasan, dan pengelolaan aset kripto yang disita, termasuk *private key* dari *Controlled Cryptowallet* dan *Controlled Address*;[122]
(6) Setelah penyitaan dilakukan, penanganan aset kripto diutamakan untuk tidak mengubah bentuk atau dikonversi ke mata uang rupiah (tunai). Dalam hal aset kripto tidak terdaftar dan/atau biaya pengelolaan tanpa konversi terlalu besar, aset kripto dapat dikonversi ke mata uang rupiah (tunai) dengan atau tanpa persetujuan pemilik aset kripto;[123]
(7) Aset kripto, baik yang sudah maupun tidak dikonversi, beserta *Controlled Cryptowallet* dan *Controlled Address* ditempatkan di ruangan khusus dalam ruang barang bukti dan dilakukan pengawasan secara berkala oleh pejabat yang menyelenggarakan tata kelola benda sitaan, barang bukti dan barang rampasan;[124]
(8) Pengurangan nilai aset kripto dan/atau biaya yang ditimbulkan akibat pemindahan dan/atau konversi aset kripto dibebankan kepada nilai aset kripto yang disita serta nantinya dinyatakan dalam surat tuntutan.[125]

Apabila dicermati, Pedoman Jaksa Agung No. 7 Tahun 2023 secara umum telah mengatur ketentuan-ketentuan serupa dengan standar internasional yang diatur oleh FATF, GAFILAT, Uni Eropa dan lembaga lainnya yang sudah dijelaskan sebelumnya. Hal ini terlihat dari

[118] Pedoman Jaksa Agung No. 7 Tahun 2023 tentang Penanganan Aset Kripto Sebagai Barang Bukti Dalam Perkara Pidana, Bab IV "Permohonan Persetujuan dan Izin Pengadilan", hal. 9 – 10.
[119] *Ibid.,* hal 4 dan 7.
[120] *Ibid.,* hal. 7.
[121] *Ibid.,* hal. 6 – 8.
[122] *Ibid.,* hal. 6 dan 11.
[123] *Ibid.,* 8.
[124] *Ibid.,* hal. 10.
[125] *Ibid.,* hal. 11.

adanya ketentuan-ketentuan yang mengacu pada prinsip umum dalam penyitaan mata uang digital, seperti pelaksanaan penyitaan yang berdasarkan izin pengadilan, penyitaan dilakukan oleh petugas yang memiliki pengetahuan dan kompetensi tertentu, dan penyimpanan hasil penyitaan melalui pemindahan ke *wallet* yang dikuasai negara. Selain itu, terdapat pula aturan yang mempertegas otoritas yang berwenang terkait pengamanan, pengawasan, dan pengelolaan mata uang digital yang disita, termasuk *private key* dari *Controlled Cryptowallet* dan *Controlled Address,* mekanisme penanganan mata uang digital yang disita, baik melalui konversi ke mata uang rupiah maupun non-konversi, hingga aturan terkait penurunan harga mata uang digital.

IV. Peluang dan Tantangan Pengaturan Mata Uang Digital Dalam Hubungannya Dengan Penegakan Hukum di Indonesia

A. Peluang dan Tantangan: Peraturan di Tatanan Pencegahan

Sebagaimana telah diuraikan dalam bagian III, perdagangan aset kripto sebagai komoditas berjangka di Indonesia saat ini diatur dan diawasi oleh Bappebti. Berdasarkan rangkaian peraturan yang dikeluarkan oleh Bappebti, berbagai aktor yang terlibat dalam perdagangan aset kripto di Indonesia adalah sebagai berikut:

Tabel5: Aktor Perdagangan Aset Kripto di Indonesia

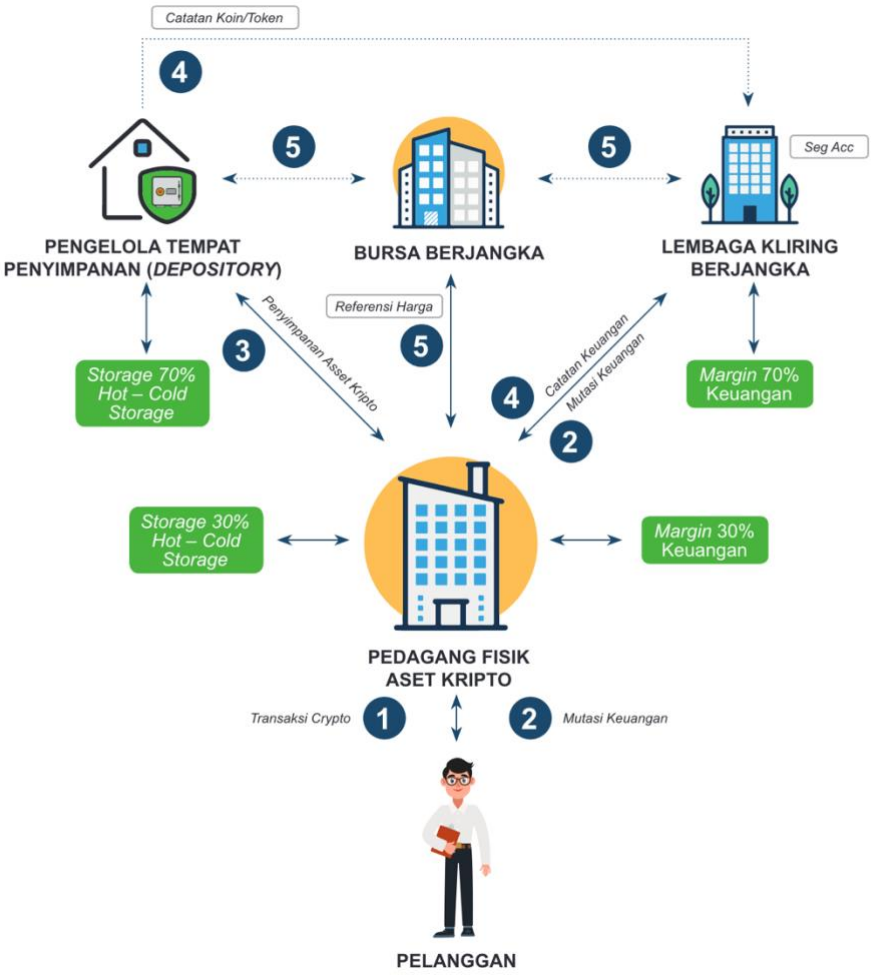
Aktor	Definisi	Keterangan
Bursa Berjangka Aset Kripto	badan usaha yang menyelenggarakan dan menyediakan sistem dan/atau sarana untuk kegiatan jual beli Komoditi berdasarkan Kontrak Berjangka, Kontrak Derivatif Syariah, dan/atau Kontrak Derivatif lainnya.	Bursa berjangka yang sudah terdaftar adalah PT Bursa Komoditi Nusantara[126]
Lembaga Kliring Berjangka	badan usaha yang menyelenggarakan dan menyediakan sistem dan/atau sarana untuk pelaksanaan kliring dan penjaminan penyelesaian transaksi Perdagangan Berjangka.	Lembaga kliring berjangka yang sudah terdaftar adalah PT Kliring Berjangka Indonesia dan PT Kliring Komoditi Indonesia[127]
Calon Pedagang Fisik Aset Kripto (*Exchanger*)	Pihak yang telah memperoleh tanda daftar dari Kepala Bappebti untuk melakukan kegiatan transaksi yang berkaitan dengan Aset Kripto baik atas nama diri sendiri dan/atau memfasilitasi Pelanggan Aset Kripto selama Bursa Berjangka Aset Kripto dan Lembaga Kliring Berjangka Aset Kripto belum terbentuk.	Saat tulisan ini ditulis, terdapat setidaknya 35 perusahaan yang terdaftar sebagai calon pedagang fisik aset kripto[128]
Pengelola Tempat Penyimpanan	pihak yang telah memperoleh persetujuan dari Kepala Bappebti untuk mengelola tempat penyimpanan Aset Kripto dalam rangka melakukan penyimpanan,	Pengelola tempat penyimpanan aset kripto yang sudah terdaftar adalah PT Tennet Depository

[126] "Bursa Berjangka Penyelenggara Perdagangan Aset Kripto", diakses melalui: https://bappebti.go.id/bursa_kripto, pada 31 Maret 2024.
[127] "Kliring Berjangka Aset Kripto," diakses melalui: https://bappebti.go.id/kliring_kripto, pada 31 Maret 2024.
[128] "Calon Pedagang Fisik Aset Kripto", Laman Resmi Bappebti, diakses melalui https://bappebti.go.id/calon_pedagang_aset_kripto pada 31 Maret 2024.

Aset Kripto (*Depository*)	pemeliharaan, pengawasan dan/atau penyerahan Aset Kripto.	Indonesia dan PT Kustodian Koin Indonesia[129]
Pelanggan Aset Kripto	pihak yang menggunakan jasa Pedagang Fisik Aset Kripto untuk membeli atau menjual Aset Kripto yang diperdagangkan di Pasar Fisik Aset Kripto.	

Adapun peran masing-masing aktor di atas dapat dipahami lebih lanjut melalui alur perdagangan aset kripto di Indonesia, yakni sebagai berikut:

Diagram ... Alur Perdagangan Aset Kripto di Indonesia



(sumber: Bappebti)

Dari alur tersebut, satu-satunya aktor yang berhadapan langsung dengan pelanggan aset kripto adalah Pedagang Fisik Aset Kripto (*exchanger*). Oleh karenanya, kewajiban untuk

[129] "Pengelola Tempat Penyimpanan Aset Kripto", diakses melalui https://bappebti.go.id/penyimpanan_kripto pada 31 Maret 2024.

menerapkan prinsip KYC, CDD, KYT dan *Travel Rules* umumnya hanya berlaku bagi *exchanger*. Oleh karenanya, pelanggan yang ingin melakukan transaksi aset kripto di Indonesia pun harus melakukan verifikasi identitas terlebih dahulu dengan *exchanger*. Setelah verifikasi identitas dilakukan, pelanggan dapat melakukan transaksi dengan melakukan penyetoran dana, dimana 70% dari dana ini disimpan oleh Lembaga Kliring dan 30% disimpan oleh *exchanger*.

Aset kripto yang telah ditransaksikan tersebut kemudian akan disimpan dengan pembagian sebagai berikut: paling sedikit 70% aset kripto disimpan oleh *depository* dan paling banyak 30% aset kripto disimpan oleh *exchanger*. Khusus bagi *exchanger*, penyimpanan aset kripto dilakukan dengan pembagian sebagai berikut: paling sedikit 70% secara *offline* (*cold wallet*), dan paling banyak 30% secara *online* (*hot wallet*).

Selain itu, *exchanger* juga berkewajiban untuk menyerahkan catatan keuangan kepada Lembaga Kliring, yang juga mencakup catatan kepemilikan aset kripto. Berdasarkan catatan keuangan ini, Lembaga Kliring kemudian menjalankan fungsi verifikasi jumlah keuangan dengan aset kripto yang ada pada Pengelola Tempat Penyimpanan (*Depository*). Berdasarkan data transaksi dari *exchanger*, Lembaga Kliring dan *depository* yang dilaporkan, Bursa Berjangka kemudian menjalankan fungsi pengawasan pasar dan mengeluarkan referensi harga yang diterapkan oleh *exchanger*.

Bappebti lebih lanjut menjelaskan bahwa bagi "*aset kripto yang telah ditransaksikan, (public dan private key) akan disimpan oleh Pedagang Komoditi Aset Kripto di depository baik yang sifatnya Hot Wallet dan Cold Wallet*".[130] Jika menautkannya dengan ulasan sebelumnya dalam Bagian II terkait jenis-jenis *wallet*, penjelasan Bappebti tersebut dapat kita maknai sebagai penggunaan *custodial wallet*, dimana *private key* pengguna disimpan secara sentral (*centralized*) oleh pihak ketiga, yang dalam hal ini merupakan *exchanger* dan/atau *depository* di Indonesia.

Hal ini akan sangat berkaitan erat dengan upaya penindakan aset kripto dalam hal terjadinya tindak pidana, karena dalam hal *custodial wallet*, APH dapat secara langsung berkoordinasi dengan *exchanger* dan/atau *depository* di Indonesia untuk mendapatkan akses terhadap aset kripto. Hal ini cukup berbeda dari penggunaan *non-custodial wallet*, dimana *private key* sepenuhnya dikelola oleh pelanggan aset kripto. Dalam situasi ini, penindakan aset kripto akan sangat bergantung pada keinginan pelanggan aset kripto untuk bekerja sama dengan aparat penegak hukum untuk menyerahkan *private key*, atau upaya aparat penegak hukum sendiri untuk menemukan *private key* tersebut. Oleh karena itu, dapat disimpulkan bahwa serangkaian peraturan Bappebti yang menerapkan *custodial wallet* di Indonesia berpeluang untuk memitigasi hambatan yang mungkin timbul dalam proses penindakan aset kripto di Indonesia.

Pembekuan Aset Kripto Berdasarkan Indikator *Red Flag*

[130] "Perdagangan Aset Kripto" (Badan pengawas Perdagangan Berjangka Komoditi (Bappebti)), 2021, hal. 12, diakses melalui: https://bappebti.go.id/resources/docs/brosur_leaflet_2001_01_10_7zwvgs5w.pdf.

Meskipun demikian, dari kasus Asabri kita dapat mengidentifikasi hambatan lain yang mengemuka dalam proses penindakan aset kripto, yakni kondisi ketika tersangka memindahkan aset kripto saat proses penyidikan berlangsung. Hal ini menggarisbawahi peran penting *exchanger* untuk dapat mengidentifikasi transaksi yang mencurigakan sebelum terjadinya tindak pidana. Sebagaimana telah diuraikan sebelumnya dalam Bagian III, melalui Rekomendasi No. 15 dan 16, FATF telah memungkinkan VASP untuk melakukan pembekuan (*freezing*) apabila terdapat transaksi yang mencurigakan berdasarkan indikator *red flag*. Adapun beberapa indikator *red flag* yang diidentifikasi oleh FATF terkait erat dengan:[131]

1. **Besaran dan frekuensi transaksi**, misalnya melakukan transaksi berulang dengan besaran kecil guna menghindari kewajiban pelaporan tertentu, melakukan transaksi ke berbagai pihak yang beroperasi di negara lain
2. **Pola transaksi yang tidak teratur, tidak biasa atau tidak lazim**, misalnya, pengguna baru yang melakukan setoran awal yang besar dan tidak sesuai dengan profil pelanggan, melakukan transaksi yang melibatkan banyak aset virtual, atau banyak akun, tanpa penjelasan bisnis yang logis.

Selanjutnya, penting untuk menyoroti apakah rekomendasi ini terintegrasi (atau tidak) dalam peraturan terkait KYT yang melekat pada *exchanger*, sebagai satu-satunya aktor yang berinteraksi langsung dengan pelanggan aset kripto di Indonesia. Peraturan Bappebti No. 8 Tahun 2021 *jo.* Peraturan Bappebti No. 13 Tahun 2022, khususnya dalam Pasal 39, mengatur bahwa sebagai bagian dari kewajiban KYT, *exchanger* harus melakukan pemantauan dan peninjauan atas transaksi aset kripto yang difasilitasinya, sehingga transaksi yang mencurigakan dapat diidentifikasi. Pemantauan dan peninjauan ini dilakukan berdasarkan *Regtech* dengan menggunakan aplikasi *blockchain analytic tools* yang berbayar atau *open source*. Lebih lanjut, Pasal 16 kemudian mengatur kewajiban *exchanger* untuk melaporkan transaksi yang mencurigakan tersebut kepada Kepala Pusat Pelaporan Analisis dan Transaksi Keuangan (PPATK).

Terdapat setidaknya dua tantangan yang dapat disoroti dalam pilihan penggunaan *Regtech* dalam proses mengidentifikasi transaksi yang mencurigakan ini, *pertama*, terkait apakah kesesuaian indikator yang digunakan aplikasi *blockchain analytic tools* dengan indikator *red flags* yang direkomendasikan FATF, dan *kedua*, upaya pengawasan yang dapat dilakukan oleh Bappebti terkait kepatuhan *exchanger* terhadap kewajiban KYT tersebut. Memastikan kesesuaian indikator *red flag* yang digunakan *exchanger* guna mengidentifikasi transaksi yang mencurigakan ini penting, karena tanpa indikator yang memadai, peluang tidak terdeteksinya transaksi mencurigakan oleh aplikasi *blockchain analytic tools* akan meningkat. Oleh karena itu, penting untuk mengadopsi indikator *red flag* transaksi aset kripto ke dalam kewajiban KYT *exchanger* di Indonesia. Hal ini tentunya harus dilakukan secara paralel dengan penguatan fungsi pengawasan Bappebti, sehingga pengawasan dilakukan tidak hanya dalam tatanan apakah *exchanger* sudah menerapkan aplikasi *blockchain analytic tools*, namun hingga pada tatanan apakah indikator yang digunakan dalam aplikasi tersebut

[131] "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing: Virtual Asset Service Providers" (FATF, September 2020), hal. 3, diakses melalui www.fatf-gafi.org/publications/fatfrecommendations/documents/VirtualAssets-Red-Flag-Indicators.html.

sudah sesuai dengan standar-standar internasional yang berlaku, khususnya yang direkomendasikan FATF.

B. Peluang dan Tantangan: Peraturan di Tatanan Penindakan

Pada bab sebelumnya, telah dijabarkan bahwa Indonesia saat ini baru memiliki 1 (satu) buah aturan yang mengatur tentang penindakan terhadap mata uang digital yang berkaitan dengan tindak pidana, yaitu Pedoman Jaksa Agung No. 7 Tahun 2023. Aturan tersebut juga telah mengatur ketentuan-ketentuan serupa dengan standar-standar internasional, baik yang diatur oleh FATF, GAFILAT, Uni Eropa, maupun lembaga lainnya, dengan mengacu pada prinsip umum dalam penyitaan mata uang digital dan mempertegas otoritas yang berwenang terkait pengamanan, pengawasan, dan pengelolaan mata uang digital yang disita. Namun demikian, masih terdapat beberapa catatan yang perlu diperhatikan dari Pedoman Jaksa Agung No. 7 Tahun 2023 tersebut, yang juga berpotensi menjadi tantangan dalam tindakan penegakan hukum atas mata uang digital yang terkait dengan tindak pidana, antara lain:

(1) Pedoman Jaksa Agung No. 7 Tahun 2023 merupakan aturan internal dari Kejaksaan, sehingga hanya bersifat mengikat bagi penegak hukum di bawah lembaga kejaksaan. Padahal, proses penyitaan mata uang digital dapat terjadi sejak proses penyidikan di mana kejaksaan hanya berwenang melakukan penyidikan dalam perkara-perkara tertentu[132], sedangkan fungsi penyidikan secara umum dilaksanakan oleh penyidik kepolisian dan Penyidik Pegawai Negeri Sipil (PPNS)[133]. Dengan kondisi tersebut, aturan-aturan dalam Pedoman Jaksa Agung No. 7 Tahun 2023 berpotensi untuk tidak diterapkan pada setiap tindak pidana yang dapat melibatkan mata uang digital, khususnya yang penyidikannya tidak dilakukan oleh kejaksaan;
(2) Pedoman Jaksa Agung No. 7 Tahun 2023 hanya mengatur prosedur penyitaan bagi mata uang digital yang tersentralisasi (*centralized*) dan menyebutkan secara eksplisit bahwa tindakan tersebut tidak dapat dilakukan untuk mata uang digital yang terdesentralisasi (*decentralized*). Padahal, salah satu ciri khas dari mata uang digital yang digunakan sebagai celah untuk melakukan kejahatan adalah sifat *decentralized* dari mata uang digital. Lebih dari itu, standar-standar yang dijelaskan sebelumnya telah mengatur bahwa penyitaan mata uang digital juga dapat dilakukan terhadap mata uang digital yang *decentralized*, yaitu melalui VASP (atau Pedagang Fisik Aset Kripto atau Pengelola Tempat Penyimpan Aset Kripto dalam konteks Indonesia) apabila mata uang digital dan *private key* disimpan oleh VASP (*custodial wallet*) dan penyitaan seluruh perangkat penyimpanan data yang berpotensi menyimpan informasi terkait *wallet*, *private key* atau *seed words* dalam hal mata uang digital dan *private key* tidak disimpan dalam *wallet* milik VASP dan dikuasai langsung oleh pemilik mata uang digital (*non-custodial wallet*);
(3) Pedoman Jaksa Agung No. 7 Tahun 2023 masih berpatokan pada tindakan penyitaan mata uang digital dan pemindahannya ke *Controlled Cryptowallet* yang harus dilakukan oleh DEFR, terlebih untuk mata uang digital yang *centralized.* Padahal, menurut standar

[132] Menurut peraturan perundang-undangan Indonesia, Kejaksaan hanya berwenang untuk melakukan penyidikan atas tindak pidana dalam UU No. 26 Tahun 2000 tentang Pengadilan Hak Asasi Manusia dan UU No. 31 Tahun 1999 *jo.* UU No. 20 Tahun 2001 tentang Pemberantasan Tindak Pidana Korupsi. Lihat UU No. 16 Tahun 2004 *jo.* UU No. 11 Tahun 2021 tentang Kejaksaan, Pasal 30 ayat (1) huruf d beserta penjelasan.

[133] UU No. 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP), Pasal 1 angka 1 *jo.* Pasal 6 ayat (1).

yang dijabarkan sebelumnya, tindakan pemblokiran/penyitaan terhadap mata uang digital *centralized* tidak membutuhkan bantuan DEFR dan dapat langsung dilakukan oleh penegak hukum dengan perintah kepada otoritas pusat dari mata uang digital tersebut berdasarkan izin pengadilan untuk memblokir/menyita dan memindahkan mata uang digital milik pelaku ke *Controlled Cryptowallet*. Bantuan DEFR dalam penyitaan mata uang digital justru pada dasarnya dibutuhkan dalam penyitaan mata uang digital yang *decentralized* dan bersifat *non-custodial wallet*, yang belum diatur dalam aturan ini, karena akan melibatkan perangkat-perangkat elektronik yang berpotensi menyimpan informasi terkait mata uang digital dan membutuhkan keahlian DEFR untuk penanganannya[134].

Berdasarkan hal-hal tersebut, dapat disimpulkan bahwa kondisi aturan penindakan mata uang digital yang terkait dengan tindak pidana masih berbeda dengan aturan-aturan pencegahannya. Apabila aturan-aturan terkait pencegahan pelibatan mata uang digital dalam kejahatan telah sesuai dengan standar-standar internasional, Indonesia belum memiliki aturan yang cukup untuk dapat melakukan penindakan terhadap mata uang digital yang berkaitan dengan tindak pidana, khususnya dalam konteks pemblokiran atau penyitaan. Oleh karena itu, Indonesia masih membutuhkan aturan-aturan terkait mata uang digital, khususnya mekanisme hukum acara pidana terkait penyitaan/pemblokiran mata uang digital, agar Indonesia memiliki aturan yang lebih komprehensif terkait penanganan mata uang digital yang berkaitan dengan tindak pidana. Beberapa ketentuan yang perlu diperhatikan dan diatur terkait hal itu antara lain:

(1) **Mengatur ketentuan penindakan mata uang digital yang terkait dengan tindak pidana, khususnya pemblokiran atau penyitaan, dalam aturan hukum acara pidana di tingkat undang-undang**. Hal ini diperlukan untuk membentuk suatu mekanisme baku penindakan mata uang digital yang terkait dengan kejahatan yang akan berlaku untuk semua jenis tindak pidana dan bagi seluruh penegak hukum mengingat beragamnya institusi penegak hukum di Indonesia yang memiliki kewenangan untuk melakukan penindakan tersebut, mulai dari kepolisian, kejaksaan, hingga PPNS dalam kejahatan-kejahatan tertentu seperti lingkungan hidup, kehutanan, perikanan, dll[135]. Dengan aturan dalam hukum acara pidana ini, para penegak hukum tersebut tidak mempraktikkan penindakan mata uang digital yang terkait dengan tindak pidana secara berbeda-beda dalam setiap tindak pidana, sehingga terdapat kepastian hukum mengenai hukum acara penindakan mata uang digital yang terkait dengan tindak pidana di Indonesia.

    Selain dibutuhkan untuk menciptakan kepastian hukum, pengaturan penindakan mata uang digital di tingkat undang-undang juga diperlukan untuk menjamin keselarasan tindakan penindakan tersebut dengan prinsip HAM. Perlu dipahami bahwa tindakan pemblokiran atau penyitaan pada dasarnya merupakan bentuk pelanggaran terhadap hak atas privasi dan harta benda/barang yang dimiliki warga negara, yang telah diatur

[134] Hal ini dikarenakan fungsi utama DEFR adalah menangani perangkat elektronik guna mencari bukti elektronik yang tersimpan di dalam perangkat tersebut. Lihat *ISO 27037: Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence*, hal. 2.

[135] Muhammad Tanziel Aziezi dan Arsil, *Asesmen Sistem Peradilan Pidana di Indonesia,* (Jakarta: Kemitraan Partnership, 2023), hal. 76.

sebagai bagian dari prinsip HAM, baik dalam konstitusi Indonesia[136], UU HAM[137], dan aturan HAM internasional[138]. Dengan kata lain, tindakan pemblokiran atau penyitaan merupakan bentuk pembatasan penikmatan hak atas privasi dan barang milik warga negara yang dilakukan oleh negara, sehingga pelaksanaannya perlu tunduk pada aturan-aturan pembatasan HAM yang diperbolehkan agar tindakan-tindakan tersebut tidak dilakukan secara sewenang-wenang. Mengacu pada hal tersebut, mengingat salah satu syarat pembatasan HAM adalah diaturnya pembatasan tersebut dalam undang-undang pada hukum nasional, maka **sudah sepatutnya aturan penindakan mata uang digital tersebut diatur dalam hukum acara pidana di tingkat undang-undang**.

(2) Beberapa ketentuan umum yang perlu diatur dengan mengacu pada standar-standar internasional yang sudah dijabarkan sebelumnya, setidak-setidaknya antara lain:
   (a) Penyitaan atau pembekuan mata uang digital harus dilakukan berdasarkan izin pengadilan. Dengan kata lain, setiap penegak hukum yang ingin melakukan penyitaan/pembekuan terhadap mata uang digital harus mengajukan izin atau mendapatkan perintah dari pengadilan terlebih dahulu sebelum penyitaan/pembekuan dilakukan. Izin atau perintah pengadilan untuk melakukan penyitaan/pembekuan harus mencantumkan identitas pihak yang akan dikenakan tindakan penyitaan/pembekuan;
   (b) Seluruh mata uang digital yang telah disita harus ditransfer ke *wallet* yang sesuai dengan jenis setiap mata uang digital milik atau yang dikelola oleh negara/pemerintah guna mencegah pelaku atau pihak lain mengambil atau mengalihkan mata uang digital tersebut sebelum proses hukum selesai dilakukan;
   (c) Seluruh informasi terkait tindakan penyitaan/pembekuan beserta besar atau jumlah mata uang digital yang disita dan *wallet* tempat menampung mata uang digital yang disita harus dicantumkan dalam berita acara penyitaan sebagaimana dimaksud dalam Pasal 75 KUHAP;

(3) Mengatur bahwa penyitaan/pembekuan mata uang digital dilakukan dalam 3 (tiga) tahap, yaitu: (i) perencanaan; (ii) pelaksanaan; dan (iii) pasca penyitaan;

(4) Mengatur bahwa beberapa hal yang perlu dilakukan penegak hukum pada tahap perencanaan, antara lain:
   (a) Mengidentifikasi jenis mata uang digital yang akan disita/dibekukan beserta sistem transaksi dan metode penyimpanannya guna mengetahui pihak yang akan dikenakan penyitaan/pembekuan serta *wallet* yang dibutuhkan untuk menampung mata uang digital yang akan disita/dibekukan;
   (b) Dalam hal penegak hukum telah mengetahui sistem transaksi dan metode penyimpanan mata uang digital yang akan disita/dibekukan, maka penegak hukum mengajukan izin penyitaan/pembekuan ke pengadilan dengan ketentuan sebagai berikut:
      - Apabila transaksi mata uang digital tersebut dilakukan secara terpusat/*centralized* oleh suatu otoritas administratif pusat, maka penegak hukum meminta pengadilan untuk menerbitkan perintah pembekuan atau

[136] Undang-undang Dasar Negara Republik Indonesia 1945, Pasal 28G ayat (1).

[137] Undang-undang No. 39 Tahun 1999 tentang Hak Asasi Manusia, Pasal 29 ayat (1).

[138] Deklarasi Universal Hak Asasi Manusia (DUHAM), Pasal 17 ayat (2). Lihat juga *International Covenant on Civil and Political Rights* (ICCPR)/Kovenan Internasional Hak-hak Sipil dan Politik (KIHSP), *General Assembly Resolution No. 2200A (XXI),* 16 Desember 1966, Pasal 17 ayat (1).

penyitaan mata uang digital kepada otoritas pusat tersebut untuk kemudian membekukan dan mentransfer mata uang digital ke alamat atau *wallet* yang dikuasai negara;

- Apabila transaksi mata uang digital dilakukan secara terdesentralisasi dan mata uang digital serta *private key* disimpan oleh Pedagang Fisik Aset Kripto atau Pengelola Tempat Penyimpan Aset Kripto (*custodian wallet*), maka penegak hukum meminta pengadilan untuk menerbitkan perintah pembekuan mata uang digital kepada Pedagang Fisik Aset Kripto atau Pengelola Tempat Penyimpan Aset Kripto tersebut untuk kemudian membekukan dan mentransfer mata uang digital ke alamat atau *wallet* yang dikuasai negara;
- Apabila transaksi mata uang digital dilakukan secara terdesentralisasi dan mata uang digital dan *private key* tidak disimpan dalam *wallet* milik Pedagang Fisik Aset Kripto atau Pengelola Tempat Penyimpan Aset Kripto (*non-custodial wallet*), maka:
    - Penegak hukum perlu meminta izin ke pengadilan untuk menyita seluruh perangkat penyimpanan data yang ditemukan saat penggeledahan, seperti komputer, telepon seluler, *hard disk* portabel, CDR, DVDR, *memory stick*, *flashdisk*, atau barang-barang lain yang berpotensi menyimpan informasi terkait *wallet*, *private key* atau *seed words* yang dapat memberikan akses penegak hukum kepada mata uang digital, seperti *wallet* perangkat keras yang menyimpan *private key* pada perangkat portable, seperti *pen drive* atau dicetak di kertas;
    - Penegak hukum perlu mempertimbangkan untuk meminta izin pengadilan agar dapat langsung melakukan penyitaan mata uang digital dan mentransfer mata uang digital tersebut ke *wallet* milik pemerintah apabila perangkat penyimpan informasi mata uang digital dalam kondisi tidak terkunci dan aktif;

(c) Dalam hal penegak hukum telah memperoleh izin pengadilan, maka penegak hukum perlu segera menyiapkan *wallet* yang dikuasai negara untuk menerima transfer mata uang digital yang akan disita sesuai dengan jenis mata uang digital tersebut;

(5) Mengatur beberapa hal yang perlu dilakukan penegak hukum pada tahap pelaksanaan, antara lain:

(a) Melakukan penyitaan terhadap mata uang digital sesuai dengan jenis mata uang digital atau *wallet* penyimpan mata uang digital tersebut dan mentransfer mata uang digital yang disita ke *wallet* yang dikuasai negara;

(b) Khusus untuk penyitaan terhadap mata uang digital yang *decentralized* dan disimpan dengan metode *non-custodial wallet*, tindakan penyitaan mata uang digital dilakukan oleh personel yang memiliki keahlian dan keterampilan untuk melakukan penyitaan tersebut terhadap berbagai jenis *wallet* mata uang digital beserta mekanisme keamanannya;

(c) Penegak hukum dapat mengisolasi pemilik mata uang digital dan semua orang lain yang hadir selama proses penyitaan berlangsung untuk mencegah mereka terhubung ke Internet atau melakukan kontak dengan dunia luar hingga penyitaan selesai;

(d) Apabila *wallet* ditemukan dalam keadaan tidak diblokir, maka penegak hukum berwenang melakukan penyitaan dan mentransfer mata uang digital yang disita ke *wallet* yang dikuasai negara secara langsung sesuai dengan izin dari pengadilan;

(e) Apabila penegak hukum menemukan perangkat yang menyimpan *wallet*, namun *wallet* tersebut diblokir dan penegak hukum tidak menemukan kata sandi yang diperlukan untuk mengaksesnya, maka penegak hukum menyita perangkat yang berisi *wallet* tersebut dengan tindakan-tindakan seperti pada penanganan bukti elektronik. Penegak hukum kemudian perlu melakukan tindakan investigasi yang relevan sesegera mungkin untuk mendapatkan kata sandi dan menyita mata uang digital;

(f) Apabila akses kepada *wallet* tersebut tidak dapat diperoleh atau *wallet* ditemukan kosong setelah dibuka, penegak hukum dapat mengidentifikasi nilai dari mata uang digital yang akan disita melalui *blockchain* dan melakukan penyitaan aset lain yang nilainya setara dengan mata uang digital tersebut;

(6) Mengatur bahwa penegak hukum wajib menuliskan seluruh informasi terkait tindakan penyitaan/pembekuan beserta besar atau jumlah mata uang digital yang disita dan *wallet* tempat menampung mata uang digital yang disita dalam berita acara penyitaan sebagaimana dimaksud dalam Pasal 75 KUHAP setelah penyitaan dilakukan;

(7) Menentukan mekanisme pengelolaan mata uang digital yang sudah disimpan dalam *wallet* milik negara atau pemerintah dengan alternatif-alternatif, antara lain:

(a) **Tetap menyimpan mata uang digital dalam bentuk yang sama ketika penyitaan dilakukan sampai putusan dijatuhkan**. Dalam hal mekanisme ini dipilih sebagai metode pengelolaan aset, maka aturan ini perlu diikuti dengan beberapa ketentuan antara lain:

- Menyimpan mata uang digital dalam *cold wallet*;
- Menyimpan kata sandi, *private key*, *seed words*, pin, dan alamat mata uang digital dalam file teks pada folder khusus untuk setiap mata uang digital yang disita pada perangkat penyimpanan eksternal yang harus tetap *offline* di lokasi aman tertentu sampai diperlukan oleh penegak hukum;
- Menunjuk pejabat tertentu untuk menyimpan perangkat yang berisi informasi kata sandi, *private key*, *seed words*, pin, dan alamat mata uang digital dan membatasi akses ke perangkat tersebut;
- Penegak hukum dapat menunjuk suatu Pedagang Fisik Aset Kripto atau Pengelola Tempat Penyimpan Aset Kripto yang dapat dipercaya untuk mengelola mata uang digital apabila penegak hukum tidak memiliki struktur keamanan siber yang dapat diandalkan untuk penyimpanan mata uang digital.

(b) **Mengkonversi mata uang digital ke dalam mata uang fiat sesegera mungkin atau dalam jangka waktu tertentu setelah penyitaan dilakukan**. Dalam hal mekanisme ini dipilih sebagai metode pengelolaan aset, maka aturan ini perlu diikuti dengan ketentuan yang memberikan kewenangan penegak hukum melakukan penjualan terhadap mata uang digital tersebut, baik secara langsung, maupun melalui lelang umum, dengan selalu mengupayakan nilai maksimal dari penjualan tersebut. Konversi tersebut juga dapat dilakukan dengan kesepakatan dengan VASP yang memiliki spesialisasi dalam pertukaran mata uang digital untuk melakukan konversi mata uang digital tersebut menjadi mata uang fiat;

(c) Keputusan terkait tindakan atas mata uang digital diambil **berdasarkan pendapat tertulis dari pemilik mata uang digital**, apakah ia lebih memilih mata uang digital tersebut disimpan dalam keadaan aslinya atau dikonversi menjadi mata uang fiat.

(8) Mengingat banyaknya pihak yang dapat terlibat dalam penindakan mata uang digital yang terkait dengan tindak pidana, diperlukan suatu kerja sama dan peran yang kuat dari lembaga-lembaga di bawah negara yang terkait pengelolaan dan pengawasan mata uang digital serta instansi-instansi penegak hukum, seperti *National Cryptocurrency Enforcement Team* (NCET) dan *Digital Asset Coordinator* (DAC) *Network* di Amerika Serikat. Di Indonesia, hal ini dapat dilakukan dengan membentuk kerja sama atau unit khusus yang berisi lembaga-lembaga yang berwenang terkait penindakan mata uang digital yang terkait dengan tindak pidana, yang setidak-tidaknya meliputi Otoritas Jasa Keuangan (OJK) sebagai pihak yang berwenang mengatur, mengelola, dan mengawasi perdagangan mata uang digital serta instansi-instansi penegak hukum.

V. Penutup

A. Kesimpulan

Penggunaan mata uang digital menjadi salah satu dampak dari berbagai upaya digitalisasi yang menyasar banyak sektor termasuk keuangan dan perbankan. Kripto menjadi salah satu mata uang digital yang mengalami peningkatan masif dalam hal jumlah pengguna termasuk nilai transaksi, baik di tingkat nasional maupun global. Meningkatnya penggunaan kripto sangat dipengaruhi dengan keunikannya yang membawa berbagai kemudahan, seperti kemampuan melakukan transaksi dengan jangkauan global, penyelesaian transaksi yang cepat dan tidak dapat diubah, serta penggunaan alamat dan nama samaran. Namun, di saat yang sama keunikan kripto tersebut juga membawa risiko tersendiri. Ketergantungan

terhadap penggunaan energi fosil, serta dibutuhkannya alokasi energi dan sumber daya yang sangat besar dalam menopang proses kerja dari teknologi *blockchain* yang menyokong kripto, berimplikasi pada kerusakan lingkungan dan semakin parahnya dampak dari krisis iklim. Ditambah lagi kripto juga memiliki risiko penyalahgunaan dalam tindak pidana seperti pencucian uang, penipuan, hingga peretasan.

Kejahatan asal yang melibatkan kripto pun beragam, mulai dari perdagangan narkotika, perdagangan orang, pendanaan terorisme, hingga kejahatan lingkungan. Dari berbagai kejahatan tersebut, kripto sebagai mata uang digital dapat memainkan peran yang berbeda-beda. Mulai sebagai alat pembayaran dan cara memfasilitasi pelaksanaan kejahatan, untuk menyembunyikan aktivitas keuangan terlarang, termasuk sebagai sarana pencucian uang dengan melakukan proses penambangan untuk membentuk koin digital baru menggunakan aset hasil aktivitas ilegal.

Kerentanan kripto untuk disalahgunakan dalam pelaksanaan kejahatan sesungguhnya sudah mendapatkan respon dengan dibentuknya sejumlah regulasi baik di tingkat internasional maupun di Indonesia. Pada tingkat internasional, langkah umum dalam pencegahan kejahatan yang melibatkan mata uang digital telah tertuang dalam rekomendasi FATF nomor 15 dan 16 pada dokumen Pencegahan dan Penindakan Kejahatan Pencucian Uang dan Pendanaan Terorisme. Sedangkan dalam ranah penindakan, FATF pada tahun 2019 telah membentuk pedoman penyitaan, pembekuan, dan perampasan mata uang digital yang tertuang dalam *Guidance on Financial Investigations Involving Virtual Assets* di tahun 2019, dan ada pula pedoman investigasi, identifikasi penyitaan, dan perampasan mata uang digital yang dikeluarkan oleh negara-negara anggota FATF kawasan Amerika Latin di tahun 2021.

Di kancah nasional, upaya pemerintah untuk mengatur pencegahan dan penindakan kejahatan yang melibatkan mata uang digital juga telah tampak. Hal ini dapat diidentifikasi dari keberadaan sejumlah regulasi yang secara spesifik menyasar aset kripto atau mata uang digital yang tengah berkembang luas. Di antaranya adalah Peraturan Menteri Perdagangan Nomor 99 Tahun 2018 Tentang Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto, yang kemudian juga diturunkan melalui dua aturan teknis dalam bentuk Peraturan Bappebti Nomor 5 Tahun 2019 dan Nomor 7 Tahun 2020. Dalam mekanisme pencegahan, peraturan-peraturan tersebut telah mengakomodir aspek-aspek penting pencegahan pelibatan mata uang digital dalam kejahatan sebagaimana dimuat dalam rekomendasi FATF nomor 15 dan 16. Serangkaian peraturan Bappebti yang menerapkan *custodial wallet* di Indonesia berpeluang untuk memitigasi hambatan yang mungkin timbul dalam proses penindakan aset kripto di Indonesia.

Berbeda dengan upaya pencegahan yang sudah dituangkan dengan baik melalui pembentukan regulasi di atas. Penanganan tindak pidana yang melibatkan kripto khususnya mencakup penyitaannya di Indonesia masih minim diatur. Ditambah lagi kurangnya pengetahuan serta pengalaman aparat penegak hukum tentang aset kripto dan cara menanganinya, juga turut menghambat proses penindakan yang dapat dilakukan. Saat ini hanya ada satu regulasi terkait penindakan kejahatan yang melibatkan mata uang digital, yaitu Pedoman Jaksa Agung Nomor 7 Tahun 2023 Tentang Penanganan Aset Kripto Sebagai Barang Bukti dalam Perkara Pidana. Peraturan ini dipandang belum cukup, sebab hanya

dapat mengikat bagi penegak hukum di bawah lembaga kejaksaan dan tidak mengatur prosedur penyitaan mata uang digital yang terdesentralisasi.

B. Rekomendasi

Berbagai kemudahan dan efisiensi yang dihadirkan oleh mata uang digital harus diiringi dengan upaya yang memadai untuk memitigasi risiko penyalahgunaannya. Sebab, jika tidak dilakukan, maka kecanggihan dan keunikan dari mata uang digital termasuk kripto justru akan berbalik menjadi aspek yang membawa lebih banyak kerugian dibanding keuntungan. Untuk itu, kami merekomendasikan sejumlah hal yang diharapkan dapat berkontribusi pada pengembangan dan perbaikan upaya penanganan kejahatan yang melibatkan kripto, di antaranya:

1. Memasukan ketentuan mengenai penindakan terhadap mata uang digital yang terkait dengan tindak pidana ke dalam revisi Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Khususnya, untuk mengatur hal-hal terkait penyitaan dan/atau pemblokiran, mulai dari tahapan perencanaan, pelaksanaan, hingga pasca penyitaan, dan upaya paksa lainnya yang diperlukan seperti penggeledahan, penyimpanan, dan perampasan;
2. Memperluas substansi pengaturan dengan tidak hanya menyasar aset kripto yang tersentralisasi, tetapi juga aset kripto yang terdesentralisasi yang berkaitan dengan tindak pidana;
3. Peningkatan pengetahuan dan kemampuan teknis aparat penegak hukum mengenai seluk beluk mata uang digital dan kripto, termasuk mekanisme penanganannya selama proses peradilan (penggeledahan, penyitaan, penyimpanan, perampasan, dll), serta kerentanan yang dimiliki;
4. Kolaborasi multipihak yang intensif dengan melibatkan aparat penegak hukum dengan kepakaran di bidang intelijen, keuangan dan perbankan, serta ahli dari aktor yang berada dalam ekosistem kripto seperti namun tidak terbatas pada *exchangers*, *trading platform*, dan *wallet providers*.

Daftar Pustaka

A. Buku / Jurnal

Alzoubi, Yehia Ibrahim, dan Alok Mishra. 2023. *"Green Blockchain – A Move towards Sustainability".* Amsterdam: Elsevier.

Gatteschi, Valentina, dkk. 2019. *"Technology of Smart Contracts"*. *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*. Cambridge: Cambridge University Press.

Lamport, Leslie. 1998. "*The Part-Time Parliament", ACM Transactions on Computer Systems* 16, no. 2

Natarajan, Harish, dkk. 2017. *"Distributed Ledger Technology (DLT) and Blockchain: FinTech Note No. 1".* Washington: World Bank.

Suripeddi, Mani Karthik Suhas, dkk. 2021. *"Blockchain and GDPR – A Study on Compatibility Issues of the Distributed Ledger Technology with GDPR Data Processing". Journal of Physics: Conference Series* 1964, no. 4. Bristol: IOP Publishing.

Tran, Duc A, dkk. 2022. "*Handbook on Blockchain Vol. 194*": Springer International Publishing.

Tuyisenge, Marie Jeanne. 2021. "Blockchain Technology Security Concerns: Literature Review". Uppsala: Uppsala Universitet.

Yanuar, Muh Afdal. 2022. "Risiko dan Posibilitas Penyalahgunaan Aset Kripto dalam Kejahatan Pencucian Uang". Majalah Hukum Nasional Vol. 52, No. 2. Jakarta: Badan Pembinaan Hukum Nasional Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia.

B. Publikasi

Aziezi, Muhammad Tanziel, dan Arsil. 2023. *"Asesmen Sistem Peradilan Pidana di Indonesia".* Jakarta: Kemitraan Partnership.

Bostwick, Lisa, dkk. 2023. "*Managing Seized and Confiscated Assets: A Guide for Practitioners".* Washington: World Bank.

Chainalysis. 2023. *"The 2023 Crypto Crime Report".* Diakses melalui: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf.

Cybercrime Programme Office of the Council of Europe (C-PROC). 2021. "*Guide On Seizing Cryptocurrencies".* Bucharest: C-PROC.

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

European Central Bank. 2015. "*Virtual Currency Schemes: A Further Analysis".* Diakses melalui: https://data.europa.eu/doi/10.2866/662172.

Evangelista, Alessio D, dkk. 2022. "*Cryptoasset Seizures and Forfeitures: US and UK Enforcement Overview*". Diakses melalui: https://www.skadden.com/insights/publications/2022/09/cryptoasset-seizures-and-forfeitures

Financial Action Task Force (FATF). 2015. "*Guidance for a Risk-based Approach: Virtual Currencies"*. France: FATF Secretariat.

Financial Action Task Force (FATF). 2023. "*Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers".* France: FATF Secretariat.

Financial Action Task Force (FATF). 2020. "*Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing".* France: FATF Secretariat.

Financial Action Task Force (FATF). 2020. "*Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing: Financial and Non-financial Sectors".* France: FATF Secretariat.

Financial Action Task Force (FATF). 2020. "*Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing: Virtual Asset Service Providers".* France: FATF Secretariat.

Financial Action Task Force (FATF). 2014. "*Virtual Currencies Key Definitions and Potential AML/CFT Risks".* France: FATF Secretariat.

Financial Action Task Force (FATF). 2023. "*International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations*". France: FATF Secretariat.

Financial Action Task Force of Latin America (GAFILAT). 2021. "*Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets".* Buenos Aires: GAFILAT.

Houben, Robby, dan Alexander Snyers. 2018. *"Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion".* Diakses melalui: https://www.ppatk.go.id/backend/assets/uploads/20170911141103.pdf.

International Organization of Securities Commissions. 2023. *"Policy Recommendations for Crypto and Digital Asset Markets".* Diakses melalui: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf.

Nakamoto, Satoshi. 2023. *"Bitcoin: A Peer-to-Peer Electronic Cash System"*. Diakses melalui: https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf.

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

Schwarz, Nadine, dkk. 2021. "*Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations"*. Washington: International Monetary Fund.

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

Tim National Risk Assessment Indonesia. 2015. "Penilaian Risiko Indonesia Terhadap Tindak Pidana Pencucian Uang". Diakses melalui: https://www.ppatk.go.id/backend/assets/uploads/20170911141103.pdf.

Transparency International Russia. 2023. *"Anonymity For Sale: The Thriving Black Market Of Crypto-To-Fiat Mules"*. Diakses melalui: https://ti-russia.org/wp-content/uploads/2023/10/epaycrypto_.pdf.

United States Department of Justice. 2022. "*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.

United States Department of Justice. 2023. "*Asset Forfeiture Policy Manual 2023".* Washington: U.S. Department of Justice.

United States Department of Justice. 2022. "*Pers Release: Justice Department Announces Report on Digital Assets and Launches Nationwide Network.* Diakses melalui:

https://www.justice.gov/opa/pr/justice-department-announces-report-digital-assets-and-launches-nationwide-network.

C. Artikel Elektronik

Bakti Kominfo. "Ciri-ciri Komputer Terinfeksi Ransomware & Cara Mengatasinya". Diakses melalui: https://www.baktikominfo.id/id/informasi/pengetahuan/ciri-ciri_komputer_terinfeksi_ransomware_cara_mengatasinya-750.

Batubara, Putranegara. 2022. "Aset Kripto Indra Kenz Rp35 Miliar Bakal Disita Bareskrim". Diakses melalui: https://www.idxchannel.com/economics/aset-kripto-indra-kenz-rp35-miliar-bakal-disita-bareskrim

Bestari, Novina Putri. 2021. "Saat Cuci Uang di Bitcoin Jadi Modus Baru Korupsi Asabri". Diakses melalui: https://www.cnbcindonesia.com/tech/20210420232119-37-239412/saat-cuci-uang-di-bitcoin-jadi-modus-baru-korupsi-asabri.

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

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

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

CNBC Indonesia. 2023. "Rafael Cuci Uang Miliaran Pakai Bitcoin, Ini kata PPATK!", diakses melalui: https://www.cnbcindonesia.com/news/20230512113504-4-436827/rafael-cuci-uang-miliaran-pakai-bitcoin-ini-kata-ppatk.

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

Damayanti, Aulia. 2024. "OJK Catat Transaksi Kripto Naik Hampir Rp 70 T dalam Sebulan", diakses melalui: https://finance.detik.com/fintech/d-7337892/ojk-catat-transaksi-kripto-naik-hampir-rp-70-t-dalam-sebulan.

Diah, Dini. 2023. "Mengenal Aset Kirpto: Pengertian, Kekurangan, dan Kelebihannya", diakses melalui: https://koran.tempo.co/read/ekonomi-dan-bisnis/483403/mengenal-aset-kripto-pengertian-kekurangan-dan-kelebihannya.

Hakim, Jefferson. 2024. "Langkah Maju Kejaksaan dalam Penyitaan Aset Kripto". Diakses melalui: https://www.hukumonline.com/berita/a/langkah-maju-kejaksaan-dalam-penyitaan-aset-kripto-lt65b9ac6bc31c8/?page=1.

Indodax Academy. 2022. "Kumpulan: Cara Trading Crypto," Belajar Jual Bitcoin Beli Bitcoin | Indodax Academy". Diakses melalui: https://indodax.com/academy/trading-di-indodax/.

Kementerian Perdagangan RI. "Bappebti Targetkan Transaksi Kripto Rp800 Triliun pada 2024". Diakses melalui: https://www.kemendag.go.id/berita/pojok-media/bappebti-targetkan-transaksi-kripto-rp800-triliun-pada-2024.

Kumparan. 2024. “Gagal Jadi Crazy Rich, Peretas Kripto Pekanbaru Ditangkap & Kekayaannya Disita”. Diakses melalui: https://kumparan.com/kumparannews/gagal-jadi-crazy-rich-peretas-kripto-pekanbaru-ditangkap-and-kekayaannya-disita-21xBpj9LqAl/1.

Kurylo, Benjamin. 2024. “Explainer: What is Environmental Crime?”. Diakses melalui: https://earth.org/explainer-what-is-environmental-crime/.

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

Megarani, Amandra. 2022. “Nilai Kejahatan Lingkungan Rp4.074 Triliun”. Diakses melalui: https://www.forestdigest.com/detail/1626/kejahatan-lingkungan

Pradianto, Aldo. 2023. “Hot Wallet: Jenis, Kelebihan, & Perbedaan dengan Cold Wallet”. Diakses melalui: https://indodax.com/academy/hot-wallet/.

Purwanto, Antonius. 2022. “Mata Uang Kripto: dari Sejarah Awal hngga Regulasi di Indonesia”, diakses melalui: https://kompaspedia.kompas.id/baca/paparan-topik/mata-uang-kripto-dari-sejarah-awal-hingga-regulasi-di-indonesia

Kementerian Perdagangan RI. 2023. “Bappebti Catat Pelanggan Aset Kripto Tembus 18,25 Juta”, diakses melalui: https: //www.kemendag.go.id/berita/pojok-media/bappebti-catat-pelanggan-aset-kripto-tembus-1825-juta.

Kemp, Simon. 2023. *“Digital 2023 Deep-dive: Blockchain’s Roadblocks*”. Diakses melalui: https://datareportal.com/reports/digital-2023-deep-dive-blockchains-roadblocks.

Kontan. 2024. “Potensi Pasar Menjanjkan, Transaksi Kripto di Indonesia meningkat”, diakses melalui: https://investasi.kontan.co.id/news/potensi-pasar-menjanjikan-transaksi-kripto-di-indonesia-meningkat.

Pamela. 2022. “Ini Perbedaan Custodial Wallet Dan Non-Custodial Wallet Pada Crypto!”. Diakses melalui: https://kripto.ajaib.co.id/perbedaan-custodial-wallet-dan-non-custodial-wallet/.

Peter, Shenna. 2024. *“Indonesian Crypto Exchanges Blame Dramatic Drop in Trading Volumes Partly on High Taxes”.* Diakses melalui: https://www.coindesk.com/policy/2024/01/17/indonesian-crypto-exchanges-blame-dramatic-drop-in-trading-volumes-partly-on-high-taxes/.

Pusat Data dan Sistem Informasi Kementerian Perdagangan Indonesia. 2024. “Bappebti Targetkan Transaksi Kripto Rp800 Triliun pada 2024”. Diakses melalui: https://www.kemendag.go.id/berita/pojok-media/bappebti-targetkan-transaksi-kripto-rp800-triliun-pada-2024.

Pusat Pelaporan dan Analisa Transaksi Keuangan. 2022. “Optimalisasi Pengembalian Aset & Keuangan Negara: PPATK Perkuat Analisis & Pemeriksaan Transaksi Keuangan”. Diakses melalui: https://www.ppatk.go.id/siaran_pers/read/1188/optimalisasi-pengembalian-aset-keuangan-negara-ppatk-perkuat-analisis-pemeriksaan-transaksi-keuangan.html.

Safitri, Kiki. dan Aprilia Ika. 2023. “Jumlah Investor Kripto di Indonesia Masuk 7 Besar Dunia”, diakses melalui, https://money.kompas.com/read/2023/12/22/170000726/jumlah-investor-kripto-di-indonesia-masuk-7-besar-dunia.

Saujana, Panca. 2021. “1700 BTC, Jaksa Jerman: Mana Password Dompet Bitcoin-nya?”. Diakses melalui: https://blockchainmedia.id/1700-btc-jaksa-jerman-mana-password-dompet-bitcoin-nya/.

Sigia, Stefano. 2020. “Environmental Crimes and Money Laundering”. Diakses melalui: https://pideeco.be/articles/environmental-green-crimes-aml-money-laundering/

Thorpe, James. 2022. “US$ 8.6 Billion Worth of Cryptocurrency Laundered by Cybercriminals in 2021”, diakses melalui: https://internationalsecurityjournal.com/cryptocurrency-laundered-in-2021/.

United Nations University. 2023. “UN Study Reveals the Hidden Environmental Impacts of Bitcoin: Carbon is Not the Only Harmful By-product”. Diakses melalui: https://unu.edu/press-release/un-study-reveals-hidden-environmental-impacts-bitcoin-carbon-not-only-harmful-product.

D. Pedoman / Perundangan

Undang-Undang Dasar Negara Republik Indonesia 1945

Deklarasi Universal Hak Asasi Manusia (DUHAM)

Kovenan Internasional Hak-hak Sipil dan Politik

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP)

Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi

Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia

Undang-Undang Nomor 26 Tahun 2000 tentang Pengadilan Hak Asasi Manusia

Undang-Undang Nomor 20 Tahun 2001 tentang Perubahan Atas Undang-Undang Nomor 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi

Undang-Undang Nomor 16 Tahun 2004 tentang Kejaksaan Republik Indonesia

Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan

Undang-Undang Nomor 11 Tahun 2021 tentang Perubahan Atas Undang-Undang Nomor 16 Tahun 2004 tentang Kejaksaan Republik Indonesia

Undang-Undang Nomor 4 tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan

Peraturan Menteri Perdagangan Republik Indonesia Nomor 99 Tahun 2018 Tentang Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto (*Crypto Asset*)

Peraturan Bappebti Nomor 3 Tahun 2020 tentang Perubahan Ketiga Peraturan Bappebti Nomor Nomor 5 Tahun 2019 tentang Ketentuan Teknis Penyelenggaraan Pasar Fisik Aset Kripto (*Crypto Asset*) di Bursa Berjangka.

Peraturan Bappebti Nomor 13 Tahun 2022 tentang Perubahan Atas Peraturan Bappebti Nomor 8 Tahun 2021 tentang Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (*Crypto Asset*) di Bursa Berjangka

Peraturan Bappebti Nomor 4 Tahun 2023 Tentang Perubahan Atas Peraturan Bappebti Nomor 11 Tahun 2022 Tentang Penetapan Daftar Aset Kripto yang Diperdagangkan di Pasar Fisik Aset Kripto.

Pedoman Jaksa Agung Nomor 7 Tahun 2023 Tentang Penanganan Aset Kripto Sebagai Barang Bukti Dalam Perkara Pidana.