

Regulasi Kejahatan Siber Berbasis Aset Kripto dalam Hukum Pidana Indonesia

M. Nanda Setiawan*, Halida Zia, Chindi Oeliga Yensi Afita

Fakultas Ilmu Sosial, Hukum dan Humaniora, Program Studi Ilmu Hukum, Universitas Muara Bungo

Jl. Lintas Sumatera Sungai Binjai, Kampus A Universitas Muara Bungo, Kabupaten Bungo

*Correspondence: Setiawannanda007@gmail.com

Article Info	Abstract
Keywords: Regulating; Crypto Asset; Cybercrime; Criminal Law. Submitted: 11-08-2026 Revised: 18-09-2026 Accepted: 13-10-2026 Published: 14-10-2026	<i>The rapid development of blockchain technology and the cryptocurrency ecosystem over the past decade has generated a new criminal landscape that transcends conventional jurisdictional boundaries. Indonesia, as the country with the fourth-largest internet user population in the world and a rapidly growing crypto market in Southeast Asia, digital transformation accelerated by the COVID-19 pandemic has expanded the attack surface for cybercriminals, leading to a significant surge in digital asset investment fraud, crypto-based money laundering, Bitcoin-ransom ransomware attacks, and terrorism financing through blockchain networks. Global indicators of money laundering via crypto assets reached USD 8.6 billion (approximately IDR 139 trillion) in 2022, with some cases involving Indonesian-based perpetrators. Against this backdrop, Indonesia's criminal law framework anchored in the Electronic Information and Transactions Law (ITE Law), the National Criminal Code (Law No. 1 of 2023), and the Anti-Money Laundering Law has not fully kept pace with the complexity of crimes based on decentralized technology. This study aims to analyze the extent to which Indonesia's criminal law regulations are responsive to cybercrimes involving digital assets and blockchain, identify existing normative gaps, and formulate evidence-based policy recommendations drawing on comparative legal analysis with the United States, European Union, Japan, and Singapore. Using a normative juridical approach and comparative law techniques, this study concludes that while UU P2SK 2023 and POJK No. 27/2024 represent progress, Indonesia still requires specific legislation on digital asset crimes, enhanced blockchain forensic capacity among law enforcement agencies, and a more systematic international cooperation framework.</i>
Kata Kunci:	Abstrak
Regulasi; Kejahatan Siber; Aset Kripto; Hukum Pidana.	Perkembangan teknologi <i>blockchain</i> dan ekosistem <i>cryptocurrency</i> dalam satu dekade terakhir telah melahirkan lanskap kejahatan yang melampaui batas yurisdiksi konvensional. Indonesia, sebagai negara dengan populasi pengguna internet terbesar keempat di dunia dan pasar kripto yang tumbuh pesat di Asia Tenggara, berada di persimpangan dua kenyataan ini transformasi digital yang dipercepat oleh pandemi COVID-19 memperluas ruang gerak pelaku kejahatan siber, sehingga kasus penipuan investasi aset digital, pencucian uang via kripto, serangan ransomware, dan pendanaan terorisme melalui <i>blockchain</i> melonjak signifikan. Indikasi pencucian uang melalui aset kripto secara global mencapai USD 8,6 miliar pada tahun 2021, sebagian di antaranya melibatkan pelaku berdomisili di Indonesia. Menghadapi fenomena ini, kerangka hukum pidana Indonesia yang berpijak pada UU ITE, KUHP Nasional (UU No. 1 Tahun 2023), dan UU Tindak Pidana Pencucian Uang belum sepenuhnya mampu menjangkau kompleksitas kejahatan berbasis teknologi terdesentralisasi. Penelitian ini bertujuan menganalisis sejauh mana regulasi hukum pidana Indonesia responsif terhadap kejahatan siber berbasis aset digital, mengidentifikasi celah normatif yang ada, serta merumuskan rekomendasi kebijakan melalui perbandingan hukum dengan Amerika Serikat, Uni Eropa, Jepang, dan Singapura. Dengan pendekatan yuridis normatif, penelitian ini menyimpulkan bahwa meski UU P2SK Tahun 2023 dan POJK No. 27 Tahun 2024 merupakan langkah maju yang konkret, Indonesia masih memerlukan undang-undang khusus kejahatan aset digital, penguatan kapasitas forensik <i>blockchain</i>, dan kerangka kerja sama internasional yang lebih sistematis.

PENDAHULUAN

Revolusi digital telah mengubah tidak hanya cara manusia berkomunikasi dan berbisnis, tetapi juga cara kejahatan dilakukan, disembunyikan, dan disebarluaskan. Di antara berbagai inovasi teknologi yang muncul, sistem *blockchain* dan mata uang kripto (*cryptocurrency*) menempati posisi yang paling kompleks secara hukum: di satu sisi menawarkan efisiensi transaksi dan demokratisasi layanan keuangan; di sisi lain menghadirkan infrastruktur yang berpotensi dimanfaatkan sebagai medium kejahatan lintas batas yang sulit dideteksi dan dituntut.¹

Indonesia, sebagai negara dengan populasi pengguna internet terbesar keempat di dunia dan pasar kripto yang tumbuh pesat di Asia Tenggara, berada di persimpangan dua kenyataan ini.² Selama periode pandemi COVID-19 (2020–2022), jumlah serangan siber mengalami lonjakan signifikan seiring masifnya pergeseran aktivitas sosial dan ekonomi ke ranah daring. PPATK mengungkap dugaan pencucian uang melalui aset kripto yang nilainya terus meningkat, sementara laporan internasional mencatat bahwa nilai kripto yang dicuci secara global mencapai USD 8,6 miliar pada tahun 2021 saja. Kasus pembobolan Pusat Data Nasional Sementara (PDNS) pada Juni 2024 oleh ransomware *Brain Cipher* dengan tuntutan tebusan USD 8 juta menjadi alarm keras bagi kedaulatan siber nasional.³

Merespons tantangan tersebut, pemerintah Indonesia mengambil langkah progresif melalui Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK) yang mengamankan peralihan pengawasan aset kripto dari Bappebti ke OJK, resmi berlaku Peraturan OJK Nomor 23 Tahun 2025. Namun, perubahan kelembagaan tersebut belum secara otomatis menjawab kebutuhan akan instrumen hukum pidana yang mampu menjerat pelaku kejahatan yang memanfaatkan ekosistem kripto. Kajian yang secara komprehensif mempertemukan analisis kriminologis, normatif-yuridis, dan komparatif dalam satu bingkai penelitian masih langka dalam diskursus akademik hukum Indonesia.⁴

Berdasarkan latar belakang tersebut, tiga permasalahan utama yang dijawab dalam penelitian ini adalah: bagaimana teknologi *blockchain* dan *cryptocurrency* dimanfaatkan sebagai instrumen kejahatan siber; sejauh mana kerangka hukum pidana Indonesia mampu menanggulangi kejahatan berbasis kripto; dan apa yang dapat dipetik dari regulasi negara-negara maju untuk memperkuat sistem hukum pidana Indonesia.

METODE

1. Jenis Penelitian

Penelitian ini menggunakan pendekatan yuridis normatif (*normative legal research*), yakni metode yang memusatkan analisis pada norma hukum tertulis, asas-asas hukum, dan doktrin melalui studi kepustakaan (*library research*).

2. Pendekatan Penelitian

Empat pendekatan diterapkan secara simultan: (1) pendekatan perundang-undangan, menelaah hierarki regulasi dari KUHP, UU ITE, UU TPPU, UU P2SK, hingga POJK 23/2025; (2) pendekatan konseptual, menggunakan doktrin hukum pidana dan teori regulasi sebagai pisau analisis; (3) pendekatan historis, menelusuri perkembangan regulasi kripto dari era Permendag No. 99 Tahun 2018 hingga rezim OJK saat ini; dan (4) pendekatan perbandingan, memperhadapkan sistem regulasi Indonesia dengan empat negara rujukan.

¹ Dwiki Putra Perkasa, “Analisis Hukum Kejahatan Ekonomi Digital *Cryptocurrency* Sebagai Instrumen *Money Laundering* di Indonesia,” *Journal of Artificial Intelligence and Digital Business*, Vol. 4, No. 2 (2025): 5474–78, <https://doi.org/https://doi.org/10.31004/riggs.v4i2.1466>.

² Supaphorn Akkapin Fadilah, Deny Susanto, “*Traditional Decriminalization in a Digital World: Reconstructing Criminal Policy towards Bitcoin-Based Money Laundering in the Era of Decentralized Finance*,” *Journal Evidence Of Law*, Vol. 4, No. 2 (2025): 753–62, <https://jurnal.erapublikasi.id/index.php/JEL>.

³ Nur Lutfie, Umi Laili, dan Muhammad Saifi, “Legalistas *Cryptocurrency* Dalam Perspektif Hukum Ekonomi Syariah,” *Jurnal Ilmu Sosial & Hukum Al-Zayn: Jurnal Ilmu Sosial & Hukum*, Vol. 3, No. 3 (2025): 3875–85, <https://doi.org/https://doi.org/10.61104/alz.v3i4.1853>.

⁴ Tantimin Abdurrahman Alhakim, “*The Legal Status of Cryptocurrency and Its Implications for Money Laundering in Indonesia*,” *Padjadjaran Journal of Law*, No. 5 (2024): 231–53, <https://doi.org/https://doi.org/10.22304/pjih.v11n2.a4>.

3. Sumber Data

Sumber data seluruhnya berupa data sekunder: bahan hukum primer (peraturan dan putusan pengadilan), bahan hukum sekunder (buku teks, jurnal ilmiah, laporan resmi lembaga negara), dan bahan hukum tersier (kamus dan ensiklopedia hukum).

4. Teknik Pengumpulan Data

Data dikumpulkan melalui studi literatur (library research), dokumentasi resmi, serta penelusuran artikel jurnal dan berita terkait.

5. Teknik Analisis Data

Dalam metode penelitian yuridis normatif, analisis bahan hukum dapat dilakukan dengan berbagai pendekatan, termasuk yuridis, normatif, dan deskriptif. Berikut adalah penjelasan masing-masing metode analisis:⁵

a. Analisis Yuridis

Analisis ini berfokus pada kajian terhadap norma hukum yang berlaku, baik dalam peraturan perundang-undangan maupun dalam praktik penerapannya. Dengan Pendekatan Menggunakan metode interpretasi hukum seperti gramatikal, sistematis, historis, dan teleologis.⁶

b. Analisis Normatif

Meneliti hukum sebagai norma atau sistem aturan yang mengatur masyarakat, dengan berfokus pada peraturan tertulis. Dengan Pendekatan Melakukan studi terhadap peraturan hukum, asas hukum, dan konsep hukum yang berlaku.⁷

c. Analisis Deskriptif

Analisis yang bertujuan memberikan gambaran tentang suatu peraturan hukum atau fenomena hukum tertentu. Dengan Pendekatan Menggunakan data dari peraturan hukum, putusan pengadilan, dan literatur untuk menjelaskan bagaimana hukum diterapkan dalam kasus nyata. Ketiga pendekatan ini sering digunakan secara bersamaan dalam penelitian hukum untuk memberikan pemahaman yang lebih komprehensif terhadap suatu isu hukum. Analisis data dilakukan secara kualitatif dengan menelaah analisis Kejahatan Siber Dan Blockchain: Tinjauan Regulasi Terhadap Aset Digital Dan *Cryptocurrency* Di Indonesia Dalam Perspektif Hukum Pidana Dilakukan Secara Kualitatif Dengan Metode Interpretasi Sistematis.

HASIL

Karakteristik *Blockchain* Dan Tantangannya Bagi Hukum Pidana

Blockchain adalah teknologi buku besar terdistribusi (*distributed ledger technology*/DLT) yang mencatat setiap transaksi dalam blok-blok data yang saling terhubung secara kriptografis, tersimpan di ribuan *node* di seluruh dunia tanpa otoritas sentral. Dari sudut pandang penegakan hukum pidana, teknologi ini menghadirkan paradoks: seluruh transaksi bersifat permanen dan dapat diaudit, namun identitas di balik alamat *wallet* bersifat pseudonim. Pelaku kejahatan yang terampil dapat memecah dan memindahkan dana kripto melalui ratusan transaksi lintas *wallet* teknik yang dalam konteks pencucian uang disebut *layering* untuk mengaburkan jejak asalnya.⁸

Kunci untuk menembus anonimitas ini adalah forensik *blockchain* (*blockchain forensics*): kombinasi analisis kriptografi, *graph analysis*, dan *cluster analysis* untuk menelusuri aliran dana antar-*wallet*. Platform analitik seperti Chainalysis dan Elliptic mampu menghasilkan laporan forensik yang dapat digunakan sebagai bukti di pengadilan.⁹ Namun, kemampuan aparat penegak hukum Indonesia dalam memanfaatkan teknologi ini masih sangat terbatas sebuah kesenjangan kapasitas yang menjadi

⁵ Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Jakarta: Rajawali Pers, 2001), hlm.17.

⁶ Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana, 2017), hlm. 89.

⁷ Johnny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif* (Malang: Bayumedia Publishing, 2006), hlm. 97.

⁸ <https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report>, diakses pada 13 juni 2026

⁹ Nurkhalisah Seri Mughni Sulubara, Viridya Tasril, "Volume 2025 Legal Protection Of Cybercrime Crimes From Ransomware Attacks And Evaluation Of The Cyber Security And Resilience Bill 2025 In Indonesia ' S Defense," *DE LEGA LATA: Jurnal Ilmu Hukum*, Vol. 10, (2025): 287-97, <https://doi.org/10.30596/dll.v10i2.25786>.

hambatan struktural paling signifikan dalam penanganan kejahatan kripto di Tanah Air.¹⁰ POJK No. 23 Tahun 2025 merespons sebagian tantangan ini dengan secara tegas melarang perdagangan kripto berfitur *untraceable transaction* seperti Monero dan ZCash di bursa Indonesia.¹¹

Tipologi Kejahatan Siber Berbasis Kripto di Indonesia

Pertama, penipuan investasi kripto dan ICO ilegal. Skema *Ponzi* berbasis kripto dan *exit scam* melalui *Initial Coin Offering* (ICO) fiktif merupakan bentuk kejahatan yang paling masif menjangkau korban di Indonesia.¹² Pelaku menciptakan antusiasme publik melalui kampanye media sosial, mengumpulkan dana investor, lalu menghilang setelah dana terkumpul modus yang dikenal sebagai *rug pull*.¹³ Minimnya literasi aset digital di masyarakat dan lemahnya mekanisme KYC (*Know Your Customer*) pada banyak platform membuat kejahatan ini relatif mudah dilakukan dan korbannya terus bertambah.

Kedua, tindak pidana pencucian uang (TPPU) melalui cryptocurrency. Proses pencucian uang berlangsung melalui tiga fase: *placement* (konversi dana haram ke kripto), *layering* (pemindahan lintas ratusan *wallet* dan jaringan *blockchain* berbeda), dan *integration* (konversi kembali ke aset nyata). Modus yang semakin canggih melibatkan penggunaan *mixer*, *tumbler*, dan broker over-the-counter (OTC) yang minim pengawasan untuk memutus jejak asal-usul dana.¹⁴ PPATK menjadikan transaksi kripto sebagai prioritas pemantauan dan menyusun *Operational Alert* penyalahgunaan aset kripto untuk berbagai tindak pidana termasuk narkoba, korupsi, perjudian, dan terorisme.¹⁵

Ketiga, serangan ransomware bermuatan kripto. Dalam serangan ransomware, pelaku mengenkripsi data korban dan menuntut tebusan dalam kripto sebagai syarat pemberian kunci dekripsi. Pilihan kripto sebagai medium tebusan dilatari oleh sulitnya memblokir transaksi kripto dibandingkan transfer bank konvensional.¹⁶ Kasus PDNS yang diserang *Brain Cipher* (evolusi Lockbit 3.0) pada Juni 2024 melumpuhkan 210 instansi pemerintah dengan tuntutan tebusan USD 8 juta¹⁷, mengekspos secara dramatis kerentanan infrastruktur digital nasional sekaligus mengungkap ketiadaan protokol hukum yang jelas terkait penanganan aset kripto dalam situasi tebusan siber.

Keempat, pendanaan terorisme. *Cryptocurrency* menjadi alternatif yang semakin diminati jaringan terorisme karena anonimitas, kecepatan, dan kemampuan transaksi lintas batas tanpa

¹⁰ Tiara Putri dan Dwi Nurfauziah Ahmad, "Inadequate Cryptocurrency and Money Laundering Regulations in Indonesia (Comparative Law of US and Germany)," *Yustisia Jurnal Hukum*, Vol. 12, No. 2 (2023): 129–52, <https://doi.org/10.20961/yustisia.v12i2.71835>.

¹¹ Krisna Bramantyo Ajil et al., "Strengthening Indonesia's Cryptocurrency Regulation to Combat Money Laundering: A Comparative Analysis of Canada and South Korea's Approaches," *Research Horizon* 0696, No. 2 (2025): 427–36, <https://doi.org/https://doi.org/10.54518/rh.5.2.2025.596>.

¹² Iqbal Nusantara dan Al Goni, "A LEGAL REVIEW OF THE HANDLING OF MONEY LAUNDERING CRIMINAL ACTS ORIGINATING FROM BITCOIN-BASED INVESTMENT CRIMES," *Akrab Juara : Jurnal Ilmu-ilmu Sosial*, Vol. 11, No. 2 (2026): 24–33, <https://doi.org/https://doi.org/10.58487/akrabjuara.v11i2.2784>.

¹³ Asyam Shobir Muyassar, Arief Fitriyanto, dan Jessika Nurhidayah, "PLATFORM-EMBEDDED ENFORCEMENT IN CRYPTOCURRENCY REGULATION: RETHINKING TAXATION AND ANTI-MONEY LAUNDERING IN INDONESIA 'S CROSS-BORDER LEGAL CONTEXT PENEGAKAN HUKUM YANG TERTANAM DALAM PLATFORM PADA REGULASI KRIPTO: MENIMBANG ULANG PAJAK DAN ANTI-PENC," *Multidisciplinary Indonesian Center Journal (MICJO)*, Vol. 2, No. 4, (2025): 4333–41, <https://doi.org/https://doi.org/10.62567/micjo.v2i4.1251> Submitted:

¹⁴ Rita Komalasari dan Cecep Mustafa, "Prosecutor 's Role in Prosecuting Cryptocurrency -Related Transnational Crimes Peran Jaksa dalam Menuntut Kejahatan Transnasional Terkait Cryptocurrency," *The Prosecutor Law Review*, Vol. 3, No. 1, (2025): 1–22, <https://doi.org/https://doi.org/10.64843/prolev.v3i1.48>.

¹⁵ I Gede Tegar dan Wingga Adi, "Regulating Cryptocurrency: Legal Responses to Emerging Financial Technologies in Global Markets," *Indonesian Journal of Law and Justice*, Vol. 3, No. 1, (2025): 1–5, <https://doi.org/https://doi.org/10.47134/ijlj.v3i1.4544>.

¹⁶ Zudan Arief Fakrulloh Pambudi, "Criminal Liability of Perpetrators in Crypto Ecosystem, the Regulatory Challenges, And Legal Voids in the Criminal Law System in Indonesia," *Majelis: Jurnal Hukum Indonesia*, Vol. 2, No. 3, (2025): 105–25, <https://doi.org/https://doi.org/10.62383/majelis.v2i3.1042>.

¹⁷ Zico Junius Fernando et al., "Crypto Mining as a Threat to Energy and the Environment from the Perspective of Criminal Law Reform," *JURNAL MEDIA HUKUM*, Vol. 18, (2025): 340–58, <https://doi.org/https://doi.org/10.18196/jmh.v32i2.27575>.

intermediary.¹⁸ PPAATK telah memasukkan risiko ini dalam Penilaian Risiko Sektor (SRA) industri perdagangan aset kripto yang diterbitkan pada 2025¹⁹, mengidentifikasi sejumlah pola transaksi mencurigakan yang mengarah pada indikasi pendanaan terorisme melalui ekosistem kripto domestik.

Kerangka Hukum Pidana Indonesia

UU ITE dan perubahannya merupakan tulang punggung hukum pidana siber. Pasal 30 melarang akses ilegal ke sistem elektronik (relevan untuk peretasan *wallet* kripto), Pasal 32 mengatur larangan perusakan informasi elektronik (relevan untuk enkripsi paksa dalam ransomware), dan Pasal 28 ayat (1) melarang penyebaran informasi menyesatkan yang merugikan konsumen andalan penuntutan penipuan ICO dan *rug pull*. Namun, UU ITE tidak memberikan definisi hukum yang jelas tentang cryptocurrency, sehingga setiap penuntutan harus dilakukan secara *ad hoc* membuka ruang ketidakpastian hukum yang cukup lebar.

KUHP Nasional (UU No. 1 Tahun 2023) mengadopsi beberapa ketentuan *cybercrime* dari UU ITE ke dalam kodeks nasional. Pasal 322 mengatur akses ilegal dengan ancaman penjara 6–8 tahun, dan Pasal 258 mengatur intersepsi tidak sah dengan ancaman penjara maksimal 10 tahun. Sementara itu, Pasal 368 KUHP lama tentang pemerasan konvensional tetap relevan untuk menjerat pelaku ransomware, meskipun tidak secara eksplisit menyebut format digital. Kodifikasi dalam KUHP Nasional memudahkan penuntutan, namun tetap belum secara spesifik mendefinisikan atau mengkategorikan kejahatan berbasis aset digital.

UU P2SK dan POJK No. 23 Tahun 2025 merupakan reformasi regulatif paling signifikan dalam sejarah pengaturan aset digital Indonesia. POJK 23/2025 memperluas definisi "aset keuangan digital", memperkuat standar KYC/AML bagi penyelenggara perdagangan, dan melarang kripto dengan fitur transaksi tidak terlacak. Namun, POJK ini pada dasarnya adalah regulasi sektoral keuangan bukan instrumen hukum pidana. POJK tidak mengatur sanksi pidana khusus, tidak menentukan mekanisme penyitaan aset kripto, dan tidak memberikan kewenangan penyidikan kepada OJK untuk kejahatan kripto yang serius. Akibatnya, terdapat kesenjangan nyata antara regulasi kehati-hatian yang semakin berkembang di satu sisi dan instrumen hukum pidana yang masih tertinggal di sisi lain.

Kripto dalam Perkara Pidana" pada Oktober 2023, menyatakan sedang menyusun pedoman bagi jaksa dalam menangani aset kripto pada seluruh tahapan perkara. Dari sisi pembuktian, bukti digital termasuk data transaksi *blockchain* diakui sebagai alat bukti sah berdasarkan Pasal 5 UU ITE jo. Pasal 235 KUHP. Namun, pemenuhan persyaratan integritas dan keaslian bukti elektronik dalam konteks *blockchain* memerlukan standar prosedur forensik yang belum sepenuhnya dimiliki aparat penegak hukum Indonesia.

Perbandingan Regulasi Internasional

Amerika Serikat menerapkan pendekatan multi-lembaga yang komprehensif: SEC mengawasi ICO sebagai sekuritas, CFTC mengawasi derivatif kripto, dan FinCEN mewajibkan platform kripto terdaftar sebagai *money service business* (MSB) dengan program AML ketat. Kejelasan klasifikasi hukum kripto di AS memberikan kepastian bagi penegak hukum dalam memilih pasal dan undang-undang yang tepat untuk setiap jenis kejahatan.

Uni Eropa mengambil pendekatan paling sistematis melalui *Markets in Crypto-Assets Regulation* (MiCA) yang berlaku seragam di 27 negara anggota sejak Juli 2023. MiCA menutup celah regulasi secara menyeluruh dengan mencakup penerbitan, perdagangan, penyimpanan, perlindungan konsumen, hingga kewajiban *whitepaper* untuk ICO dalam satu instrumen tunggal menghilangkan kemungkinan suatu kategori aset kripto "jatuh di antara kursi" karena tidak diatur satu pun regulator.

Jepang adalah negara pertama yang melegalkan *cryptocurrency* sebagai alat pembayaran melalui *Payment Services Act*, dengan Badan Layanan Keuangan (FSA) mengawasi bursa kripto secara ketat melalui kewajiban registrasi, pemisahan dana pengguna, dan standar keamanan berlapis. Tragedi Mt. Gox (2014) dan peretasan Coincheck (2018) mendorong reformasi regulatif dramatis yang kini

¹⁸ Taufiq Ramadhan et al., "Illegal Access Melalui Metode Phishing Pada Platform Transaksi Digital Cryptocurrency Dalam Perspektif KUHP Baru dan Undang-Undang ITE," *PAGARUYUANG LAW JOURNAL*, Vol. 9, No. 2, (2026): 332–46, <https://doi.org/https://doi.org/10.31869/plj.v9i2.7142>.

¹⁹ <https://grc-indonesia.com/artikel/perubahan-pengawasan-kripto-ojk-gantikan-bappebti-apadampaknya/>, diakses pada 13 juni 2026

menjadikan Jepang sebagai salah satu sistem pengawasan kripto paling ketat sekaligus paling ramah konsumen di dunia.

Singapura memposisikan diri sebagai *hub* kripto Asia Tenggara dengan model *regulatory sandbox* yang memungkinkan perusahaan fintech *blockchain* menguji inovasi di bawah pengawasan terbatas sebelum mendapat lisensi penuh. Pendekatan *pro-innovation with guardrails* MAS ini berhasil menarik investasi sekaligus menjaga integritas sistem keuangan sebuah keseimbangan yang belum berhasil dicapai oleh Indonesia.

SIMPULAN

Pertama, teknologi *blockchain* memiliki sifat ganda yang secara inheren menantang hukum pidana konvensional: permanennya transaksi memudahkan audit, namun sifat pseudonim dan kapabilitas lintas batas mempersulit identifikasi pelaku dan perampasan aset kejahatan. Empat tipologi kejahatan penipuan ICO, TPPU via kripto, ransomware, dan pendanaan terorisme masing-masing memerlukan respons hukum terspesialisasi yang tidak dapat dikelola memadai hanya dengan pasal-pasal umum yang tersedia saat ini. Kedua, meski peralihan pengawasan ke OJK melalui UU P2SK dan POJK 23/2025 merupakan kemajuan regulatif yang nyata, perubahan ini masih bersifat administratif-sektoral dan belum menyentuh dimensi hukum pidana secara substansial. Indonesia belum memiliki *lex specialis* yang secara eksplisit mengkriminalisasi perilaku berbahaya dalam ekosistem aset digital. Ketiga, perbandingan dengan AS, UE, Jepang, dan Singapura memperlihatkan Indonesia masih tertinggal dalam kejelasan klasifikasi yuridis kripto, kerangka sanksi pidana khusus, kapasitas forensik blockchain, dan mekanisme koordinasi multi-lembaga yang terstruktur.

DAFTAR PUSTAKA

Peraturan Perundang-Undangan

- Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik
Undang-Undang Nomor 8 Tahun 2010 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang
Undang-Undang Nomor 9 Tahun 2013 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pendanaan Terorisme
Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana
Undang-Undang Nomor 4 Tahun 2023 Tentang Pengembangan Dan Penguatan Sektor Keuangan
Peraturan Otoritas Jasa Keuangan Nomor 27 Tahun 2024 Tentang Penyelenggaraan Perdagangan Aset Keuangan Digital Termasuk Aset Kripto

Jurnal

- Adiyatma, S. E., & Maharani, D. F. Cryptocurrency's Control in the Misuse of Money Laundering Acts as an Effort to Maintain the Resilience and Security of the State. *Lex Scientia Law Review*, Vol. 4, No. 1, (2020) : 70–82. <https://doi.org/10.15294/lesrev.v4i1.38257>
Al Nusantara, I., et al. A Legal Review of the Handling of Money Laundering Criminal Acts Originating from Bitcoin-Based Investment Crimes. *Akrab Juara: Jurnal Ilmu-Ilmu Sosial*, Vol. 11, No. 2, (2026) : 24–33. <https://doi.org/10.58487/akrabjuara.v11i2.2784>
Alhakim, A., & Tantimin. The Legal Status of Cryptocurrency and Its Implications for Money Laundering in Indonesia. *Padjadjaran Jurnal Ilmu Hukum (PJIH)*, Vol. 11, No. 2, (2024). <https://doi.org/10.22304/pjih.v11n2.a4>
Anwar, M., et al. Legal Protection of Cybercrime Crimes from Ransomware Attacks in Indonesia. *De Legalata: Jurnal Ilmu Hukum*, Vol. 9, No. 2, (2024). <https://jurnal.umsu.ac.id/index.php/delegalata/article/view/25786>
Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Rezi. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. *Justisia: Jurnal Ilmu Hukum*, Vol. 1, No. 1, (2024) : 1-11.
Erawati, E., et al. Crypto Regulation and Anti Money Laundering in Indonesia. *Jurnal Pembangunan Hukum Indonesia (JPHI)*, Vol. 7, No. 2, (2025). <https://ejournal2.undip.ac.id/index.php/jphi/article/view/29778>
Fadilah, F., Susanto, D., & Akkapin, S. Traditional Decriminalization in a Digital World: Reconstructing Criminal Policy towards Bitcoin-Based Money Laundering in the Era of

- Decentralized Finance. *Jurnal Education and Law (JEL)*, Vol. 4, No. 2, (2025) : 753–768. <https://jurnal.erapublikasi.id/index.php/JEL/article/view/1523>
- Harianto, S., et al. Legal Protection for Crypto Asset Investors in Indonesia Within an Incomprehensive Regulatory Framework and its Implications for Legal Certainty. *Journal of Government and Social Problems (JGSP)*, Vol. 3, No. 3, (2025). <https://doi.org/10.38035/jgsp.v3i3.433>
- Komalasari, R. Prosecutor's Role in Prosecuting Cryptocurrency-Related Transnational Crimes. *The Prosecutor Law Review*, Vol. 3, No. 1, (2025). <https://doi.org/10.64843/prolev.v3i1.48>
- Mutiara, A., & Purnomo, B. Inadequate Cryptocurrency and Money Laundering Regulations in Indonesia: Comparative Law of US and Germany. *Yustisia Jurnal Hukum*, Vol. 12, No. 2, (2023). <https://jurnal.uns.ac.id/yustisia/article/view/71835>
- Pambudi, P., & Fakrulloh, Z. A. Criminal Liability of Perpetrators in Crypto Ecosystem, the Challenges and the Perspectives. *Majelis: Jurnal Hukum dan Hak Asasi Manusia*, Vol. 2, No. 3, (2024). <https://doi.org/10.62383/majelis.v2i3.1042>
- Putra Perkasa, D. Analisis Hukum Kejahatan Ekonomi Digital Cryptocurrency Sebagai Instrumen Money Laundering di Indonesia. *RIGGS: Journal of Research in Islamic Economic and Business*, Vol. 4, No. 2, (2025) : 5474–5478. <https://doi.org/10.31004/riggs.v4i2.1466>
- Saputra, D. H., & Kusumah, F. Blockchain Forensics and the Evidentiary Challenges of Crypto-Based Corruption in Developing Countries. *Indonesian Journal of Criminal Law Studies (IJCLS)*, Vol. 10, No. 2, (2025) <https://doi.org/10.15294/ijcls.v10i2.28795>
- Sioe, F. C., & Tanaya, P. E. Regulasi Hukum Cryptocurrency Pencegahan Tindak Penyalahgunaannya di Indonesia. *Jurnal Kertha Semaya*, Vol. 12, No. 6, (2024) : 1378–1392. <https://doi.org/10.24843/KS.2024.v12.i06.p02>

Laporan Resmi dan Sumber Kelembagaan

BSSN (Badan Siber dan Sandi Negara). *Laporan Insiden Siber: Ransomware Pusat Data Nasional Sementara*. Jakarta: Badan Siber dan Sandi Negara, 2024.

Website

<https://www.chainalysis.com/blog/2022-crypto-crime-report/>
<https://antikorupsi.org>
<https://kehati-jambi.kejaksaan.go.id/penanganan-aset-kripto-dalam-perkara-pidana/>
<https://ojk.go.id/id/regulasi/Pages/POJK-27-2024-AKD-AK.aspx>
<https://www.ppatk.go.id/backend/assets/uploads/20250226052005.pdf>
<https://www.ppatk.go.id/news/read/1562>