Mizaan: Journal of Sharia, Law, and Economics
e-ISSN: XXXX-XXXX
Vol. 1, No. 1, 2026, pp. 01-18

OPEN ACCESS

Crypto Crimes And Digital Assets: New Regulations In Indonesian Criminal Law

Endi Arofa*
Universitas Pamulang, Tangerang Selatan, Indonesia
dosen01978@unpam.ac.id

Tubagus Ahmad Ramadan
Universitas Pamulang, Tangerang Selatan, Indonesia
dosen02295@unpam.ac.id

DOI: 10.66277/mizaan.1.1.3

Received: 29-05-2026	Revised: 04-06-2026, 06-06-2026	Accepted: 02-07-2026

*Corresponding Author

Abstract

Indonesia's rapid integration into the global cryptocurrency ecosystem has generated systemic vulnerabilities that existing penal instruments are structurally ill-equipped to address. With more than 17 million registered crypto-asset investors and transaction volumes surpassing IDR 650 trillion by 2024, the digital financial landscape has simultaneously expanded the surface area for sophisticated crimes — including rug pulls, phishing, and illicit exchange operations — that fall outside the explicit reach of conventional criminal law. This study examines the normative construction of Indonesian criminal law in addressing crypto-asset crime, maps the doctrinal gaps within existing regulatory instruments, and proposes an adaptive legal reform model. Employing a normative-juridical methodology integrating statutory, conceptual, and comparative approaches, the analysis draws on primary, secondary, and tertiary legal materials. The findings demonstrate that current instruments remain partial, interpretive, and reliant on analogical reasoning that is epistemically in tension with the nullum crimen sine lege principle. The P2SK Law (Law No. 4 of 2023), Government Regulation No. 49 of 2024, and POJK No. 27 of 2024 jo. POJK No. 23 of 2025 have collectively reoriented the supervisory paradigm toward Digital Financial Assets (DFA) under the Financial Services Authority (OJK), yet independent criminal offense qualifications for crypto-native crimes remain absent. This study concludes that the establishment of a lex specialis governing digital asset crimes, the strengthening of institutional digital forensic capacity, and the expansion of mutual legal assistance frameworks across jurisdictions constitute an urgent tripartite reform agenda for Indonesia's national criminal justice system.

[*Integrasi cepat Indonesia ke dalam ekosistem cryptocurrency global telah menghasilkan kerentanan sistemik yang secara struktural tidak dapat ditangani* *oleh instrumen pidana yang ada. Dengan lebih dari 17 juta investor aset kripto terdaftar dan volume transaksi melampaui Rp 650 triliun pada tahun 2024, lanskap keuangan digital secara bersamaan telah memperluas area permukaan untuk kejahatan canggih — termasuk rug pull, phishing, dan operasi pertukaran ilegal — yang berada di luar jangkauan eksplisit hukum pidana konvensional. Studi ini mengkaji konstruksi normatif hukum pidana Indonesia dalam mengatasi kejahatan aset kripto, memetakan kesenjangan doktrin dalam instrumen regulasi yang ada, dan mengusulkan model reformasi hukum yang adaptif. Menggunakan metodologi normatif-yuridis yang mengintegrasikan pendekatan undang-undang, konseptual, dan komparatif, analisis ini mengacu pada materi hukum primer, sekunder, dan tersier. Temuan ini menunjukkan bahwa instrumen saat ini tetap parsial, interpretatif, dan bergantung pada penalaran analogis yang secara epistemik bertentangan dengan prinsip nullum crimen sine lege. Undang-Undang P2SK (UU No. 4 Tahun 2023), Peraturan Pemerintah No. 49 Tahun 2024, dan POJK No. 27 Tahun 2024 jo. POJK No. 23 Tahun 2025 secara kolektif telah mengarahkan kembali paradigma pengawasan ke arah Aset Keuangan Digital (DFA) di bawah Otoritas Jasa Keuangan (OJK), namun kualifikasi tindak pidana independen untuk kejahatan kripto-native masih belum ada. Studi ini menyimpulkan bahwa pembentukan lex specialis yang mengatur kejahatan aset digital, penguatan kapasitas forensik digital kelembagaan, dan perluasan kerangka kerja bantuan hukum timbal balik di seluruh yurisdiksi merupakan agenda reformasi tripartit yang mendesak untuk sistem peradilan pidana nasional Indonesia.*]

Keywords: Crypto Crime; Digital Financial Assets; Indonesian Criminal Law; Legal Vacancies; Regulatory Reform;

Introduction

The emergence of *blockchain*-based financial instruments has fundamentally disrupted the architecture of the global monetary order, generating both unprecedented transactional efficiencies and novel vectors for criminal exploitation that conventional legal systems remain structurally unprepared to address. In Indonesia, the scale of this disruption is empirically unmistakable: the number of registered *crypto*-asset investors exceeded 17 million at the end of 2023, with transaction volumes surpassing IDR 300 trillion in that year alone before escalating dramatically to more than IDR 650 trillion by 2024. According to the Chainalysis 2025 *Crypto Crime Report*, global illicit *cryptocurrency* transaction volumes reached an estimated USD 40.9 billion in 2024, with projections suggesting that figure could surpass USD 51 billion as forensic methodologies continue to identify previously unattributed addresses — a trajectory that underscores the inadequacy of reactive regulatory postures.[1]This surge in activity simultaneously exposes a wide regulatory gap for various forms of *cybercrime* that exploit the anonymity, decentralization, and

[1] Chainalysis, "2025 Crypto Crime Report," *Chainalysis Inc*, 2025.

cross-jurisdictional characteristics inherent in the *crypto* ecosystem, thus presenting a serious challenge for Indonesia's national criminal legal system that is not yet fully adaptive to digital transformation.[2]

Various modes of *crypto*-asset-based crime have developed in a structurally organized and increasingly sophisticated manner, encompassing money laundering, investment fraud, *rug pull*, *phishing*, terrorism financing, and cross-border tax crimes. The pseudonymous nature of *crypto* transactions renders perpetrator identification and judicial proof exceptionally challenging for law enforcement.[2] The *Financial Action Task Force* (FATF), in its 2023 Targeted Update on Virtual Asset Service Providers (VASPs), documented that approximately 75% of assessed jurisdictions demonstrated only partial or non-compliance with Recommendation 15 governing anti-money laundering and counter-terrorism financing for virtual assets — a systemic governance deficit that Indonesia shares.[3] This systemic weakness is compounded by the absence of dedicated investigative institutions with authority over *crypto*-sector criminal cases, leaving enforcement agencies to rely on fragmented sectoral legal instruments that are neither integrated nor comprehensively designed for the decentralized digital ecosystem.[4]

From a normative perspective, a significant legal vacuum exists within Indonesian criminal law concerning the qualification of *crypto*-based criminal acts, the classification of legal subjects within decentralized systems, and the mechanisms for confiscating digital assets as evidentiary objects. Existing provisions — including Law No. 11 of 2008 on Information and Electronic Transactions and Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering — are not architecturally designed to accommodate the complexities of the *crypto* ecosystem.[5] The *lex lata* framework's inability to provide comprehensive coverage has been observed across comparative jurisdictions: Manthovani's comparative analysis of Indonesian money laundering frameworks identified structural deficiencies in addressing *cryptocurrency*-mediated proceeds of crime, finding that analogical interpretations of financial transaction definitions are jurisprudentially fragile when applied to *blockchain*-based transfers.[6] These normative lacunae directly undermine

---

[2] Tiara Putri et al., "Inadequate Cryptocurrency and Money Laundering Regulations in Indonesia (Comparative Law of US and Germany)," *Yustisia* 12, no. 2 (2023): 129–52, https://doi.org/10.20961/yustisia.v12i2.71835.

[3] Financial Action Task Force (FATF), "Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs.," FATF-GAFI, 2023, https://www.fatf-gafi.org.

[4] Febby Mutiara Nelson et al., "Cracking the Code: Investigating the Hunt for Crypto Assets in Money Laundering Cases in Indonesia," *Journal of Indonesian Legal Studies* 9, no. 1 (2024): 89–130, https://doi.org/10.15294/jils.vol9i1.4534.

[5] Pambudi and Zudan Arief Fakrulloh, "Criminal Liability of Perpetrators in Crypto Ecosystem, the Regulatory Challenges, and Legal Voids in the Criminal Law System in Indonesia," *Majelis: Jurnal Hukum Indonesia* 2, no. 3 (2025): 105–25, https://doi.org/10.62383/majelis.v2i3.1042.

[6] Reda Manthovani, "A Comparative Analysis of Money Laundering Crimes in Indonesia through Cryptocurrency," *International Journal of Cyber Criminology* 17, no. 1 (2023): 196–210, https://doi.org/10.5281/zenodo.4766612.

victim protection and the effectiveness of law enforcement at both the investigative and prosecutorial stages.

Criminal liability attribution for *crypto*-asset crime perpetrators in Indonesia faces a further structural obstacle arising from regulatory dualism between the commodity-supervisory regime previously administered by BAPPEBTI and the financial services framework under OJK. The act of converting criminal proceeds into *crypto*-assets to obscure their origin constitutes money laundering (*tindak pidana pencucian uang*/TPPU), yet the proof thereof is subject to both technical and normative constraints rooted in institutional jurisdictional ambiguity.[7] This regulatory fragmentation has been analyzed through a polycentric governance lens by Maarif, who demonstrates that jurisdictional overlaps between BAPPEBTI and OJK prior to the P2SK Law created a form of systemic regulatory capture — wherein neither authority assumed full operational responsibility for *crypto*-sector criminal enforcement, leaving institutional gaps that organized criminal actors systematically exploited.[8] Agarwal et al. further establish that *blockchain* forensic tools integrating machine learning and chain analytics can achieve identification accuracy of 97.5% in *cryptocurrency* fraud detection, yet such technical capacities are operationally irrelevant without a corresponding normative framework that specifies the evidentiary admissibility criteria and procedural authority of the investigating agency.[9]

Significant regulatory reforms have emerged since the issuance of Law No. 4 of 2023 (the P2SK Law), which transferred supervisory authority over *crypto* assets from BAPPEBTI to OJK, subsequently operationalized through Government Regulation No. 49 of 2024. This provision was then further implemented through OJK Regulation (POJK) No. 27 of 2024 *jo.* POJK No. 23 of 2025, which reclassifies *crypto* assets as *Digital Financial Assets* (DFA) subject to Anti-Money Laundering (AML), Know Your Customer (KYC), and broader risk management compliance standards.[10] The European Union's *Markets in Crypto-Assets* Regulation (MiCA), formally adopted in May 2023 under Regulation (EU) 2023/1114 and fully implemented by December 2024, represents the world's most comprehensive attempt to establish a unified legal framework for *crypto*-asset issuers and service

---

7 I Nyoman Sucitrawan, M Arief Amrullah, and Fanny Tanuwijaya Tanuwijaya, "Money Laundering Criminal Liability Through Crypto Asset Exchange in Indonesia," *International Journal of Law, Crime and Justice* 1, no. 3 (2024): 314–21, https://international.appihi.or.id/index.php/IJLCJ/article/view/190.

8 Syamsul Maarif, "Digital Asset Enforcement Reform in Indonesia: A Polycentric Governance Approach," *Yustisia* 15, no. 1 (2026): 1–20, https://doi.org/10.20961/yustisia.v15i1.110549.

9 Udit Agarwal et al., "Blockchain and Crypto Forensics: Investigating Crypto Frauds," *International Journal of Network Management* 34, no. 2 (March 1, 2024): e2255, https://doi.org/https://doi.org/10.1002/nem.2255.

10 Jerry Peryanto et al., "Perlindungan Hukum Bagi Pengguna Cryptocurrency Menurut UU No. 4 Tahun 2023 Tentang P2SK. Legal Protection for Cryptocurrency Users According to Law No. 4 of 2023 Concerning P2SK," *Jurnal Kolaboratif Sains* 8, no. 5 (2025): 2432–46, https://doi.org/10.56338/jks.v8i5.7576.

providers — mandating transparency, authorization, and robust AML/KYC compliance obligations.[11] Indonesia's paradigm shift toward DFA oversight mirrors the foundational logic of MiCA, yet remains critically incomplete in its criminal law dimension.

The technical and cross-jurisdictional dimensions of *crypto*-crime enforcement add further complexity beyond the normative: tax regulations and AML frameworks, treated as separate regulatory domains, share a common operational architecture in digital platform infrastructure, creating exploitable gaps that criminals leverage systematically. Muyassar, Fitrijanto, and Nurhidayah have proposed the concept of *Platform-Embedded Enforcement* — integrating supervisory mechanisms directly into platform architecture in real-time — as a theoretical framework capable of addressing the limitations of conventional regulatory approaches in the digital financial era.[12]

WScholarship on *crypto*-crime regulation has evolved substantially in the past three years. Nelson et al. examined the investigative challenges of asset tracing in Indonesian money laundering cases involving *crypto*-assets, identifying evidentiary gaps in applying the TPPU framework to pseudonymous *blockchain* transactions.[13] Pambudi and Fakrulloh systematically mapped the criminal liability vacuum in Indonesia's *crypto* ecosystem, articulating the regulatory challenges and normative voids that persist despite sector-level reforms.[14] At the comparative international level, the Georgetown *Global Anti-Money Laundering Law for Crypto-Assets* study demonstrated that even advanced regulatory frameworks such as MiCA and the U.S. Bank Secrecy Act do not fully resolve the beneficial ownership opacity embedded in DeFi platforms and non-custodial wallets.[15] Gjorgjev, Ramadhan, and Dhamayana's *blockchain* forensics study further revealed that while *de-anonymization* tools can uncover transaction patterns in dark web contexts, the absence of standardized forensic protocols in national criminal procedure law — particularly in developing nations — continues to obstruct judicial proceedings.[16] What remains underexplored in the existing literature is the precise juristic mechanism through which Indonesia's

[11] European Parliament and Council of the European Union, “Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA),” *Official Journal L* 150, no. 9 (2023): 40–205.

[12] Asyam Shobir Muyassar, Arief Fitrijanto, and Jessika Nurhidayah, “Platform-Embedded Enforcement In Cryptocurrency Regulation: Rethinking Taxation And Anti-Money Laundering In Indonesia’s Cross-Border Legal Context,” *Multidisciplinary Indonesian Center Journal* (MICJO) 2, no. 4 (2025): 4333–41, https://doi.org/10.62567/micjo.v2i4.1251.

[13] Nelson et al., “Cracking the Code: Investigating the Hunt for Crypto Assets in Money Laundering Cases in Indonesia.”

[14] Pambudi and Fakrulloh, “Criminal Liability of Perpetrators in Crypto Ecosystem, the Regulatory Challenges, and Legal Voids in the Criminal Law System in Indonesia.”

[15] Francesco Paolo Patti, “Towards a Global Anti-Money Laundering Law for Crypto-Assets,” *Geo. J. Int’l L*, 2025, 697–727.

[16] Jelena Gjorgjev, M.F. Fajar Ramadhan, and Sonny Dhamayana, “Blockchain Forensics - Unmasking Anonymity in Dark Web Transactions,” *International Journal of Criminology and Sociology* 14 (2025): 68–75, https://doi.org/10.6000/1929-4409.2025.14.07.

administrative supervisory transition under the P2SK Law intersects — or fails to intersect — with the nation's penal enforcement apparatus, particularly regarding *crypto*-native offenses such as *rug pulls* and *pump-and-dump* schemes that have no explicit statutory *delik* in Indonesian criminal law. This gap constitutes the central scholarly contribution of the present study.

Based on the above, this study formulates three main research problems. First, how is the current construction of Indonesian criminal law applied in qualifying *crypto*-asset-based crimes from the aspects of legal subjects, prohibited acts, and criminal liability? Second, to what extent do regulatory updates through the P2SK Law, Government Regulation No. 49 of 2024, POJK No. 27 of 2024 *jo.* POJK No. 23 of 2025, and the ITE Law succeed in closing the legal vacuum that has constituted a systemic obstacle in handling digital asset crimes? Third, what is the ideal model for criminal law regulation of digital asset crimes in the Indonesian legal system to ensure legal certainty, victim protection, and effective law enforcement in the digital space?

This research aims to analyze in depth the normative construction of Indonesian criminal law in addressing *crypto*-asset-based crime, identify doctrinal gaps, evaluate the effectiveness of the latest regulatory framework under the P2SK Law and its implementing regulations, and formulate adaptive criminal law policy recommendations that prioritize victim protection and systemic resilience.[3] Theoretically, this research contributes to the academic discourse on digital economy criminal law and *blockchain*-responsive criminal policy. Practically, it provides normative guidance for policymakers, OJK, PPATK, law enforcement, and digital asset industry actors in understanding the applicable legal framework and designing more integrated enforcement instruments.

Methodology

This research employs a normative-juridical methodology, treating law as a prescriptive and autonomous norm system subject to systematic scholarly analysis. Given that the core inquiries concern the existence of legal vacuums, regulatory inconsistencies, and norm-incoherence among applicable instruments governing *crypto*-asset crimes, the normative approach is epistemically warranted — as emphasized by Nurhayati et al., who affirm its appropriateness for studies centered on norm systematics rather than empirical legal behavior.[1] Three integrated analytical approaches are deployed: first, the *statute approach*, through which all relevant legislation — including the P2SK Law (No. 4/2023), Government Regulation No. 49/2024, POJK No. 27/2024 *jo.* POJK No. 23/2025, Law No. 1/2024 (amended ITE Law), and Law No. 8/2010 (Money Laundering Prevention) — is examined for internal consistency and external coherence with the *crypto* ecosystem's operational realities; second, the *conceptual approach*, wherein legal constructs such as criminal liability, *Digital Financial Assets* (DFA), and *dormant liability* in decentralized systems are identified and analyzed to construct normative arguments; and third, the *comparative approach*, through which regulatory models from the United States, European Union, and relevant international frameworks — including FATF Recommendation 15 and EU MiCA — are examined as reference points for formulating an ideal Indonesian regulatory model. Wiraguna emphasizes that combining normative, comparative, and conceptual approaches within a single research frame produces more comprehensive and solution-oriented analyses of multidimensional legal problems.[17]

The data sources in this study are exclusively secondary in character, consistent with the library-research methodology of normative legal scholarship. Primary legal materials comprise regulations with binding normative force: the P2SK Law, Government Regulation No. 49/2024, POJK No. 27/2024 *jo*. POJK No. 23/2025, the Criminal Code (KUHP), the *Code of Criminal Procedure* (KUHAP), the ITE Law, and the Money Laundering Prevention Law. Secondary legal materials encompass peer-reviewed national and international legal journals, institutional reports from FATF, OJK, and PPATK, and relevant court decisions. Tertiary materials include legal dictionaries, encyclopedias, and authoritative online sources for the clarification of technical terminology. Data collection is conducted through systematic literature analysis tracing all relevant legal materials to the research problem formulation, consistent with Benuf and Azhar's methodological framework for normative legal research.[18]

Data analysis employs descriptive-qualitative methodology integrated with four legal interpretation techniques: grammatical, systematic, historical, and teleological. Each legal norm is interpreted not merely textually but also from the perspective of the *das sollen* — the normative purpose underlying its formulation — and its practical compatibility with the operational realities of *crypto*-crime. Legal construction techniques, including analogical reasoning and *argumentum a contrario*, are applied where statutory *lacunae* require bridging, while remaining attentive to the epistemological limits imposed by the *nullum crimen sine lege* principle. Results are presented in a narrative-prescriptive mode, articulating not only the existing normative condition but also constructive recommendations for Indonesian digital criminal law reform.

[17] Sidi Ahyar Wiraguna, "Metode Normatif Dan Empiris Dalam Penelitian Hukum: Studi Eksploratif Di Indonesia," *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3, no. 3 (2024), https://doi.org/10.59818/jps.v3i3.1390.

[18] Kornelius Benuf and Muhamad Azhar, "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," *Jurnal Gema Keadilan* 7, no. 1 (2020): 145–60.

The Indonesian Criminal Law Construction in Qualifying Crypto-Asset-Based Crimes

Indonesia's criminal law system confronts a profound structural challenge in addressing *crypto*-asset crime, rooted in the fundamental absence of explicit criminal qualifications that directly reference the *cryptocurrency* ecosystem. The applicable legal framework continues to rely on sectoral and partial instruments — notably Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering and the ITE Law — neither of which was architecturally designed to engage with the operational complexities of decentralized digital transactions. At the core of this structural deficit lies an epistemological tension between the *Principle of Legality* (*nullum crimen sine lege praevia*) and the judicial practice of progressive interpretation or analogy. Scholars from Oxford's *Current Legal Problems* have documented that in international criminal law contexts, progressive jurisprudence — filling normative *lacunae* through expansive interpretation — fundamentally risks subjective justice over formal legality.[19] This tension is acutely manifest in Indonesian judicial practice: while *crypto* assets such as *Bitcoin* can be categorized under the financial transaction definition in Article 1(4) of Law No. 8/2010, such application demands progressive interpretation that may compromise the foreseeability and determinacy requirements of the *nullum crimen sine lege* principle.[20]

The potential of *cryptocurrency* as a vehicle for money laundering (*tindak pidana pencucian uang*/TPPU) has substantially complicated investigative, prosecutorial, and enforcement processes across the board, because the pseudonymous transaction mechanism impedes the tracing of illicit fund flows across digital wallets.[21] The act of converting criminal proceeds into *crypto*-assets with the intent to disguise their origin juridically constitutes TPPU, yet the absence of a *lex specialis* governing *cryptocurrency*-mediated TPPU mechanisms renders law enforcement structurally ill-equipped to prosecute such cases.[22] Saputra and Kusumah's *blockchain* forensics study confirms that evidentiary challenges in *crypto*-based corruption cases in developing countries are compounded by the absence of standardized forensic protocols in national criminal procedure law, making both investigation and judicial admission of *blockchain*-derived evidence

[19] Payam Akhavan, "The Perils of Progressive Jurisprudence: The Nullum Crimen Sine Lege Principle in International Criminal Law," *Current Legal Problems* 75, no. 1 (December 1, 2022): 45–70, https://doi.org/10.1093/clp/cuac002.

[20] Dewi Asri Puanandini, "Pidana Pencucian Uang Hasil Kejahatan Siber (Cyber Crime) Melalui Mata Uang Digital (Crypto Currency)," *Jurnal Pemuliaan Hukum* 4, no. 2 (2021): 57–70, https://doi.org/10.30999/jph.v4i2.1480.

[21] Benuf and Azhar, "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer."

[22] Puanandini, "Pidana Pencucian Uang Hasil Kejahatan Siber (Cyber Crime) Melalui Mata Uang Digital (Crypto Currency)."

operationally precarious.[23] Simultaneously, the presence of *cryptocurrency* meaningfully expands opportunities for terrorism financing, while Law No. 9 of 2013 on the Prevention and Eradication of Terrorism Financing Crimes has demonstrably failed to adapt: the existing regulation positions *cryptocurrencies* solely as assets, not as means of payment, thereby generating exploitable legal loopholes for organized criminal networks.[24] This condition confirms that Indonesian criminal law on *crypto* crimes remains at the stage of analogical and interpretive norm application, and has not yet advanced to the establishment of independent, comprehensive criminal qualifications.

The Chainalysis 2024 *Crypto Crime Report* documents that illicit *cryptocurrency* transaction volumes in 2023 totaled USD 24.2 billion — representing 0.34% of total on-chain activity — while stablecoins comprised approximately 60% of all illicit transactions, reflecting a structural shift in criminal methodology that existing TPPU frameworks are wholly unprepared to address.[25] The global prevalence of *rug pull* schemes — which according to Immunefi's reports exceeded USD 100 million in documented losses in 2023 alone, with over 350 events documented globally in 2024 representing a 15% year-on-year increase — further illustrates the inadequacy of existing Indonesian criminal law frameworks that contain no explicit statutory *delik* for this category of *crypto*-native fraud.[26]

The Legal Vacuum and Its Impact on Digital Asset Law Enforcement

The legal vacuum in Indonesian digital asset crime enforcement is not solely a matter of absent norms but encompasses a more systemic conflict among existing regulatory instruments that collectively generate structural obstacles to effective enforcement. Regulatory fragmentation, asset classification ambiguity, cross-border enforcement barriers, limited digital forensic capacity, and weak inter-agency coordination constitute structural deficiencies that directly impair victim recovery, legal certainty, and market confidence in Indonesia's digital financial ecosystem. Prior to the P2SK Law, institutional dualism between BAPPEBTI and OJK generated profound normative confusion: *crypto* assets were simultaneously classified as commodities under the futures trading regime and as financial instruments with implications requiring OJK oversight — a jurisdictional bifurcation that Maarif analyzes through a polycentric governance lens as producing systemic regulatory paralysis, wherein overlapping institutional mandates left no single

[23] Dadang Herli Saputra and Fardana Kusumah, "Blockchain Forensics and the Evidentiary Challenges of Crypto-Based Corruption in Developing Countries," *Indonesian Journal of Criminal Law Studies* 10, no. 2 (2025): 615–58, https://journal.unnes.ac.id/journals/ijcls/article/view/28795.

[24] M Alief Thoifurqoni Assyamiri and Aris Hardinanto, "Penggunaan Bitcoin Dalam Cryptocurrency Terhadap Pendanaan Terorisme," *Inicio Legis* 3, no. 1 (2022): 1–17, https://doi.org/10.21107/il.v3i1.14421.

[25] Chainalysis, "2024 Crypto Crime Report," 2024.

[26] Coinlaw.io, "Rug Pulls & Ponzi Schemes in Crypto Statistics 2025: Analyzing Data and Trends.," 2025, https://coinlaw.io/rug-pulls-amp-ponzi-schemes-in-crypto-statistics/.

authority with the operational responsibility and technical capacity to investigate *crypto*-sector crimes comprehensively.[27]

From an international comparative perspective, Indonesia's enforcement challenges are not contextually isolated. Salisu, Filipov, and Pene's study on *blockchain* forensics in the age of decentralization documents that de-anonymization methodologies — including address clustering, chain analytics, and OSINT-based wallet attribution — have advanced to a technically capable stage, yet their deployment remains hampered in jurisdictions lacking both forensic infrastructure and adequate legal frameworks governing the admissibility of *blockchain*-derived evidence.[28] The EU's MiCA Regulation — the world's first comprehensive crypto-asset regulatory framework, fully implemented in December 2024 — directly addresses the beneficial ownership transparency challenge by mandating KYC and AML obligations for all *Crypto*-Asset Service Providers (CASPs), demonstrating a model of administrative-criminal integration that Indonesia's current regulatory reforms have not yet replicated.[7] Various jurisdictions additionally grapple with issues surrounding *blockchain* data protection, *smart contracts*, *Initial Coin Offerings* (ICOs), and *Decentralized Autonomous Organizations* (DAOs), all of which demand an adaptive and comprehensive legal framework capable of serving criminal law enforcement purposes.[29]

Indonesia's incapacity to establish a system enabling effective confiscation and recovery of digital assets constitutes a foundational enforcement problem, particularly when perpetrators conceal criminal proceeds in *crypto* wallets unregistered with licensed platforms. Unlike conventional assets traceable through centralized banking infrastructure, digital assets are intangible, distributed, and non-custodial — rendering the asset seizure mechanism in the *Code of Criminal Procedure* (KUHAP) directly inapplicable.[30] Aruan, Toha, and Nurdin's comparative legal analysis of digital asset confiscation frameworks establishes that Indonesia currently lacks any procedurally sound mechanism for digital asset seizure for enforcement purposes, and proposes EU Directive (EU) 2024/1260 on asset recovery and forfeiture as a paradigmatic reference, noting the structural

[27] Maarif, "Digital Asset Enforcement Reform in Indonesia: A Polycentric Governance Approach."

[28] Saminu Salisu and Velitchko Filipov, "Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation ," *International Conference on Cyber Warfare and Security* 18, no. 1 (2023): 338–47, https://doi.org/10.34190/iccws.18.1.947.

[29] Peraturan OJK, "Nomor 23 Tahun 2025 Tentang Perubahan Atas Peraturan Otoritas Jasa Keuangan Nomor 27 Tahun 2024 Tentang Penyelenggaraan Perdagangan Aset Keuangan Digital Termasuk Aset Kripto" 2 (2024): 306–12, https://ojk.go.id/id/regulasi/Pages/POJK-23-2025-Perubahan-POJK-27-Tahun-2024-tentang-Penyelenggaraan-Perdagangan-Aset-Keuangan-Digital-Termasuk-Aset-Kripto.aspx.

[30] D A KC et al., "Blockchain and Cryptocurrency: International Legal and Regulatory Challenges," in *Bloomsbury Academic* (Bloomsbury Academic, 2023), https://books.google.co.id/books?id=0U16EAAAQBAJ.

compatibility between Indonesia's civil law tradition and the EU model.[31] The SoK study on cross-border criminal investigations published in the *Journal of Cybersecurity* (Oxford) further establishes that *Mutual Legal Assistance Treaties* (MLATs) currently face critical limitations in digital asset tracing contexts due to inadequate data categorization frameworks and the operational slowness of judicial cooperation instruments relative to the speed of *blockchain* transactions.[32] These systemic deficiencies, taken together, confirm that the structural paralysis of Indonesia's digital asset enforcement framework requires not merely incremental regulatory amendment but a foundational institutional and legislative overhaul.

Regulatory Reform: The Implications of the P2SK Law, Government Regulation No. 49/2024, POJK No. 27/2024, and POJK No. 23/2025

The wave of regulatory reforms from the P2SK Law to POJK No. 23 of 2025 represents the state's systematic effort to close the legal vacuum obstructing criminal law enforcement in the digital asset sector. Law No. 4 of 2023, through Article 1(6), affirms OJK as an independent institution with functions encompassing regulation, supervision, audit, and investigation of the financial services sector, while Article 4(t) explicitly designates law enforcement in the financial sector as within the law's scope.[33] These provisions collectively confirm that *crypto* crime enforcement has been incorporated into the national financial sector law enforcement framework, transcending its earlier commodity classification. Government Regulation No. 49 of 2024 operationalizes the P2SK mandate by ending institutional dualism and reclassifying *crypto* assets as *Digital Financial Assets* (DFA), while requiring implementation of KYC, Customer Due Diligence (CDD), AML, and Counter-Terrorism Financing (CTF) standards for all digital asset trading operators.[34]

POJK No. 27 of 2024 subsequently provides normative certainty by defining the legal subjects of the *crypto* ecosystem — DFA, traders, exchanges, wallets, and trading operators — thereby resolving one of the central obstacles in determining the legal standing of parties and imposing criminal liability on illegal *crypto* business actors. The comprehensive governance of the DFA ecosystem — encompassing licensing, electronic system security, consumer fund protection, and transaction

---

[31] Albert Richi Aruan, Kurnia Toha, and Aad Rusyad Nurdin, "Digital Governance for Confiscating Crypto-Assets to Settle Tax Liabilities in Indonesia," *APTISI Transactions on Technopreneurship* 7, no. 3 (2025): 1066–79, https://doi.org/10.34306/att.v7i3.649.

[32] Fran Casino et al., "SoK: Cross-Border Criminal Investigations and Digital Evidence," *Journal OfCybersecurity*, 2022, 1–18, https://doi.org/10.1093/cybsec/tyac014.

[33] Peraturan OJK, "Nomor 23 Tahun 2025 Tentang Perubahan Atas Peraturan Otoritas Jasa Keuangan Nomor 27 Tahun 2024 Tentang Penyelenggaraan Perdagangan Aset Keuangan Digital Termasuk Aset Kripto."

[34] Peraturan Otoritas Jasa Keuangan, "Nomor 27 Tahun 2024 Tentang Penyelenggaraan Perdagangan Aset Keuangan Digital Termasuk Aset Kripto," 2024, https://peraturan.bpk.go.id/Details/323277/peraturan-ojk-no-27-tahun-2024.

reporting obligations — establishes a foundational basis for criminal law enforcement against illegal exchanges, digital investment fraud, and market manipulation.[1] The *Financial Stability Board*'s 2023 High-Level Recommendations for the regulation of *crypto*-asset activities, endorsed by the G20, similarly conclude that orderly, transparent, and AML/KYC-integrated supervisory frameworks constitute a fundamental prerequisite for effective *crypto*-crime detection and enforcement.[35]

However, a critical juristic paradox emerges from this reform architecture: while the P2SK Law, PP 49/2024, and the POJKs effectively shift the supervisory paradigm toward DFA, they remain predominantly administrative and regulatory in nature, without generating independent criminal offense qualifications. The investigative powers granted to OJK Civil Servant Investigators (*Penyidik Pegawai Negeri Sipil*/PPNS-OJK) under the P2SK Law potentially create institutional overlap — or a procedurally ambiguous bridge — with the National Police (*Polri*) cyber-crime units when *crypto*-native crimes escalate beyond administrative infractions into severe penal violations. Further improvements are introduced through POJK No. 23 of 2025, which through Article 3A expands the scope of digital criminal law objects to include digital asset *derivatives*, and through Article 1(17) opens a pathway for tracing *beneficial owners* and platform controllers — previously a blind spot in corporate criminal law enforcement in the *crypto* sector.[36] This administrative transparency mechanism, while legally significant, must be further operationalized through the doctrine of corporate criminal liability (*pertanggungjawaban pidana korporasi*): enforcement authorities need explicit evidentiary procedures for using AML and *beneficial ownership* disclosures to pierce the cryptographic veil of decentralized platform controllers and hold illegal exchange operators criminally accountable under national penal law. The *Georgetown* global AML study documents that even under MiCA, DeFi platforms operating through admin-key governance structures remain partially opaque to conventional corporate piercing doctrines, suggesting that Indonesia's corporate criminal liability instruments will require adaptation to the technical realities of decentralized platform governance.[37]

Model Ideal Regulasi Hukum Pidana Kejahatan Aset Digital di Indonesia

Beginning from an analysis of the existing legal construction and the impact of recent regulatory reforms, the ideal model for criminal law regulation of *crypto*

---

[35] Financial Stability Board, "High-Level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final Report," FSB, 2023, https://www.fsb.org/2023/07/.

[36] Peraturan OJK, "Nomor 23 Tahun 2025 Tentang Perubahan Atas Peraturan Otoritas Jasa Keuangan Nomor 27 Tahun 2024 Tentang Penyelenggaraan Perdagangan Aset Keuangan Digital Termasuk Aset Kripto."

[37] Aruan, Toha, and Nurdin, "Digital Governance for Confiscating Crypto-Assets to Settle Tax Liabilities in Indonesia."

crime in Indonesia should be constructed upon three mutually reinforcing pillars: normative certainty, integrated institutional architecture, and technology-adaptive enforcement mechanisms. The first pillar — normative certainty — necessitates the establishment of a *lex specialis* for digital asset crime as a non-deferrable legislative priority. Rather than merely enumerating *crypto*-native offenses such as *rug pull*, *pump-and-dump*, digital asset *phishing*, illegal exchanges, and *wallet* theft, the drafters of this *lex specialis* must formally codify each offense as explicit statutory *delik* (*unsur-unsur tindak pidana*) in accordance with the *nullum crimen sine lege* framework — specifying *mens rea*, *actus reus*, causation standards, victim recovery mechanisms, and proportionate criminal sanctions. Saputra and Kusumah's forensic study confirms that the absence of such statutory clarity not only frustrates prosecution but also renders judicially obtained *blockchain* evidence procedurally contestable.[11] The EU MiCA Regulation's approach — in which each category of *crypto*-asset service is matched with explicit compliance obligations that trigger both administrative and criminal consequences — offers a legislative drafting model transferable to Indonesia's civil law tradition.[38] issue further complicates codification: as Colangelo's analysis in the *Capital Markets Law Journal* (Oxford) demonstrates, DAOs do not neatly fit existing corporate or contractual legal categories, demanding that any *lex specialis* for digital asset crime explicitly address the attribution of criminal liability within DAO governance structures.[39]

The second pillar — institutional capacity — requires the establishment of specialized digital forensic investigation units within OJK, PPATK, and *Polri* cyber units, operating under clearly delineated jurisdictional workflows. International *enforcement* cooperation studies, including Daraojimba et al.'s comparative analysis of cross-border *cryptocurrency* enforcement, establish that no single national enforcement architecture can effectively address *crypto*-crime without simultaneous investment in inter-agency technical capacity and international information-sharing protocols.[40] The FATF's 2024 Fifth Targeted Update on VASP implementation further confirms that jurisdictions with materially significant VASP activity — including Indonesia — continue to experience critical gaps in VASP licensing, registration, and offshore platform oversight that can only be resolved through dedicated institutional capacity beyond the supervisory agency.[41] These specialized units must be equipped with technical competencies encompassing

---

[38] European Parliament and Council of the European Union, "Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA)."

[39] Shabir Korotana, "Decentralized Autonomous Organizations: Adapting Legal Structures and Proposing a New Model of DAOLLP," *Capital Markets Law Journal* 20, no. 3 (September 1, 2025): kmaf011, https://doi.org/10.1093/cmlj/kmaf011.

[40] Chinonso Ikegwu, Ngozi Uzougbo, and Fola Odion, "International Enforcement of Cryptocurrency Laws: Jurisdictional Challenges and Collaborative Solutions," *Magna Scientia Advanced Research and Reviews* 11 (May 13, 2024): 68–83, https://doi.org/10.30574/msarr.2024.11.1.0075.

[41] Korotana, "Decentralized Autonomous Organizations: Adapting Legal Structures and Proposing a New Model of DAOLLP."

blockchain transaction tracing, anonymous *wallet* owner identification, and digital asset confiscation — capacities whose technical dimensions are described in the *blockchain* forensics literature as requiring machine learning integration and standardized chain-of-custody protocols.[42]

The third pillar — cross-border cooperation — demands the expansion of *Mutual Legal Assistance* mechanisms specifically accommodating the trans-jurisdictional characteristics of *crypto* crime. Cross-border evidence gathering in *crypto* criminal investigations, as documented in the *Tilburg Law Review*, has seen an exponential increase in MLA requests between 2023 and 2024, yet existing MLA treaty frameworks remain operationally inadequate for the rapid freezing of assets in non-custodial, decentralized wallets.[43] The implementation of Directive (EU) 2024/1260 on asset recovery and forfeiture in the European Union — which establishes an integrated framework for tracing, freezing, and recovering criminal proceeds including digital assets — provides a particularly relevant reference point for Indonesia, given the structural parallels in civil law tradition and the comparable regulatory challenges faced.[44] The Budapest Convention's mechanisms for cross-border *cybercrime* cooperation, including harmonized offenses, MLA protocols, and 24/7 evidence-sharing networks, similarly offer institutional templates that Indonesia's ITE Law reforms should actively incorporate.[45] Through the coherent development of these three pillars, Indonesia's criminal justice system can achieve a transformation from reactive to preventive-integrative in addressing the escalating challenges of digital asset crime.

Conclusion

This research reveals that the construction of Indonesian criminal law remains normatively inadequate to address the full complexity of *crypto*-asset-based crimes, as the available legal instruments continue to operate in a partial, interpretive, and analogically dependent mode — a jurisprudential posture that is structurally in tension with the *nullum crimen sine lege praevia* principle and generates systemic legal uncertainty for both enforcement agencies and affected victims. Although the wave of regulatory reforms through the P2SK Law, Government Regulation No. 49 of 2024, and POJK No. 27 of 2024 *jo.* POJK No. 23 of 2025 has effectuated a significant paradigm shift — transitioning from commodity-based supervision under BAPPEBTI

---

42 Financial Stability Board, “High-Level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final Report.”

43 Tessa Roomen, “Cross-Border Evidence Gathering in Criminal Crypto Investigations: A Case Study of the Netherlands,” *Tilburg Law Review* 30 (November 28, 2025): 120–46, https://doi.org/10.5334/tilr.423.

44 A S Jaya and T V Widyastuti, “Legalitas Cryptocurrency Di Indonesia,” in *Penerbit NEM* (Penerbit NEM, 2022), https://books.google.co.id/books?id=yNSYEAAAQBAJ.

45 Md Hasibul Alam Ratul, Sepideh Mollajafari, and Martin Wynn, “Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution,” *Sustainability (Switzerland)* 16, no. 24 (2024), https://doi.org/10.3390/su162410885.

toward a *Digital Financial* Assets framework under OJK — the normative vacuum in the qualification of *crypto*-native criminal offenses as independent statutory *delik* (*lex specialis*) remains unresolved and operationally consequential.

The proposed three-pillar reform model — comprising (1) a *lex specialis* for digital asset crime with explicit statutory *delik* codifying offenses such as *rug pull*, digital asset *phishing*, illegal exchanges, and *pump-and-dump* schemes; (2) specialized institutional digital forensic capacity establishing clear procedural workflows among OJK's PPNS investigators, PPATK's financial intelligence analysts, and *Polri* cyber units; and (3) expanded *mutual legal assistance* frameworks that accommodate non-custodial and decentralized wallet tracing — offers a definitive structural response to the administrative-penal enforcement gap that Indonesia's current reform trajectory has not yet bridged. The long-term systemic impact of these reforms extends beyond mere law enforcement effectiveness: the establishment of a comprehensive digital asset criminal law architecture is foundational to restoring legal certainty, safeguarding investor protection, and preserving Indonesia's national market integrity within the global digital economy. Future research should specifically address the legal challenges posed by emerging decentralized architectures — including DeFi protocols and DAOs — whose governance structures of *smart contracts* and *token*-based decision-making will continue to test the jurisdictional reach of state sovereignty and the conceptual limits of criminal liability attribution in decentralized environments.

Bibliography

Agarwal, Udit, Vinay Rishiwal, Sudeep Tanwar, and Mano Yadav. "Blockchain and Crypto Forensics: Investigating Crypto Frauds." *International Journal of Network Management* 34, no. 2 (March 1, 2024): e2255. https://doi.org/https://doi.org/10.1002/nem.2255.

Akhavan, Payam. "The Perils of Progressive Jurisprudence: The Nullum Crimen Sine Lege Principle in International Criminal Law." *Current Legal Problems* 75, no. 1 (December 1, 2022): 45–70. https://doi.org/10.1093/clp/cuac002.

Aruan, Albert Richi, Kurnia Toha, and Aad Rusyad Nurdin. "Digital Governance for Confiscating Crypto-Assets to Settle Tax Liabilities in Indonesia." *APTISI Transactions on Technopreneurship* 7, no. 3 (2025): 1066–79. https://doi.org/10.34306/att.v7i3.649.

Assyamiri, M Alief Thoifurqoni, and Aris Hardinanto. "Penggunaan Bitcoin Dalam Cryptocurrency Terhadap Pendanaan Terorisme." *Inicio Legis* 3, no. 1 (2022): 1–17. https://doi.org/10.21107/il.v3i1.14421.

Benuf, Kornelius, and Muhamad Azhar. "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Jurnal Gema Keadilan* 7, no. 1 (2020): 145–60.

Casino, Fran, Claudia Pina, Pablo López-aguilar, Agusti Solanas, Constantinos Patsakis, and Edgar Batista. "SoK: Cross-Border Criminal Investigations and Digital Evidence." *Journal OfCybersecurity*, 2022, 1–18.

https://doi.org/10.1093/cybsec/tyac014.

Chainalysis. “2024 Crypto Crime Report,” 2024.

———. “2025 Crypto Crime Report.” *Chainalysis Inc*, 2025.

Coinlaw.io. “Rug Pulls & Ponzi Schemes in Crypto Statistics 2025: Analyzing Data and Trends.,” 2025. https://coinlaw.io/rug-pulls-amp-ponzi-schemes-in-crypto-statistics/.

European Parliament and Council of the European Union. “Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA).” *Official Journal L* 150, no. 9 (2023): 40–205.

Financial Action Task Force (FATF). “Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs.” FATF-GAFI, 2023. https://www.fatf-gafi.org.

Financial Stability Board. “High-Level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final Report.” FSB, 2023. https://www.fsb.org/2023/07/.

Gjorgjev, Jelena, M.F. Fajar Ramadhan, and Sonny Dhamayana. “Blockchain Forensics - Unmasking Anonymity in Dark Web Transactions.” *International Journal of Criminology and Sociology* 14 (2025): 68–75. https://doi.org/10.6000/1929-4409.2025.14.07.

Ikegwu, Chinonso, Ngozi Uzougbo, and Fola Odion. “International Enforcement of Cryptocurrency Laws: Jurisdictional Challenges and Collaborative Solutions.” *Magna Scientia Advanced Research and Reviews* 11 (May 13, 2024): 68–83. https://doi.org/10.30574/msarr.2024.11.1.0075.

Jaya, A S, and T V Widyastuti. “Legalitas Cryptocurrency Di Indonesia.” In *Penerbit NEM*. Penerbit NEM, 2022. https://books.google.co.id/books?id=yNSYEAAAQBAJ.

KC, D A, D Armstrong, D Hyde, and S Thomas. “Blockchain and Cryptocurrency: International Legal and Regulatory Challenges.” In *Bloomsbury Academic*. Bloomsbury Academic, 2023. https://books.google.co.id/books?id=0U16EAAAQBAJ.

Korotana, Shabir. “Decentralized Autonomous Organizations: Adapting Legal Structures and Proposing a New Model of DAOLLP.” *Capital Markets Law Journal* 20, no. 3 (September 1, 2025): kmaf011. https://doi.org/10.1093/cmlj/kmaf011.

Maarif, Syamsul. “Digital Asset Enforcement Reform in Indonesia: A Polycentric Governance Approach.” *Yustisia* 15, no. 1 (2026): 1–20. https://doi.org/10.20961/yustisia.v15i1.110549.

Manthovani, Reda. “A Comparative Analysis of Money Laundering Crimes in Indonesia through Cryptocurrency.” *International Journal of Cyber Criminology* 17, no. 1 (2023): 196–210. https://doi.org/10.5281/zenodo.4766612.

Muyassar, Asyam Shobir, Arief Fitrijanto, and Jessika Nurhidayah. “Platform-Embedded Enforcement In Cryptocurrency Regulation: Rethinking Taxation And Anti-Money Laundering In Indonesia’s Cross-Border Legal Context.” *Multidisciplinary Indonesian Center Journal* (MICJO) 2, no. 4 (2025): 4333–41. https://doi.org/10.62567/micjo.v2i4.1251.

Nelson, Febby Mutiara, Maria Dianita Prosperiani, Choky Risda Ramadhan, and Priska Putri Andini. “Cracking the Code: Investigating the Hunt for Crypto Assets in Money Laundering Cases in Indonesia.” *Journal of Indonesian Legal Studies* 9, no. 1 (2024): 89–130. https://doi.org/10.15294/jils.vol9i1.4534.

Pambudi, and Zudan Arief Fakrulloh. “Criminal Liability of Perpetrators in Crypto Ecosystem, the Regulatory Challenges, and Legal Voids in the Criminal Law System in Indonesia.” *Majelis: Jurnal Hukum Indonesia* 2, no. 3 (2025): 105–25. https://doi.org/10.62383/majelis.v2i3.1042.

Patti, Francesco Paolo. “Towards a Global Anti-Money Laundering Law for Crypto-Assets.” *Geo. J. Int'l L*, 2025, 697–727.

Peraturan OJK. “Nomor 23 Tahun 2025 Tentang Perubahan Atas Peraturan Otoritas Jasa Keuangan Nomor 27 Tahun 2024 Tentang Penyelenggaraan Perdagangan Aset Keuangan Digital Termasuk Aset Kripto” 2 (2024): 306–12. https://ojk.go.id/id/regulasi/Pages/POJK-23-2025-Perubahan-POJK-27-Tahun-2024-tentang-Penyelenggaraan-Perdagangan-Aset-Keuangan-Digital-Termasuk-Aset-Kripto.aspx.

Peraturan Otoritas Jasa Keuangan. “Nomor 27 Tahun 2024 Tentang Penyelenggaraan Perdagangan Aset Keuangan Digital Termasuk Aset Kripto,” 2024. https://peraturan.bpk.go.id/Details/323277/peraturan-ojk-no-27-tahun-2024.

Peryanto, Jerry, Diana W Ria Napitupulu, Paltiada Saragi, Artikel Penelitian, and Kata Kunci. “Perlindungan Hukum Bagi Pengguna Cryptocurrency Menurut UU No. 4 Tahun 2023 Tentang P2SK. Legal Protection for Cryptocurrency Users According to Law No. 4 of 2023 Concerning P2SK.” *Jurnal Kolaboratif Sains* 8, no. 5 (2025): 2432–46. https://doi.org/10.56338/jks.v8i5.7576.

Puanandini, Dewi Asri. “Pidana Pencucian Uang Hasil Kejahatan Siber (Cyber Crime) Melalui Mata Uang Digital (Crypto Currency).” *Jurnal Pemuliaan Hukum* 4, no. 2 (2021): 57–70. https://doi.org/10.30999/jph.v4i2.1480.

Putri, Tiara, Amiludin, Dwi Nurfauziah Ahmad, and Hidayatulloh. “Inadequate Cryptocurrency and Money Laundering Regulations in Indonesia (Comparative Law of US and Germany).” *Yustisia* 12, no. 2 (2023): 129–52. https://doi.org/10.20961/yustisia.v12i2.71835.

Ratul, Md Hasibul Alam, Sepideh Mollajafari, and Martin Wynn. “Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution.” *Sustainability (Switzerland)* 16, no. 24 (2024). https://doi.org/10.3390/su162410885.

Roomen, Tessa. “Cross-Border Evidence Gathering in Criminal Crypto Investigations: A Case Study of the Netherlands.” *Tilburg Law Review* 30 (November 28, 2025): 120–46. https://doi.org/10.5334/tilr.423.

Salisu, Saminu, and Velitchko Filipov. “Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation .” *International Conference on Cyber Warfare and Security* 18, no. 1 (2023): 338–47. https://doi.org/10.34190/iccws.18.1.947.

Saputra, Dadang Herli, and Fardana Kusumah. “Blockchain Forensics and the Evidentiary Challenges of Crypto-Based Corruption in Developing Countries.”

Indonesian Journal of Criminal Law Studies 10, no. 2 (2025): 615–58. https://journal.unnes.ac.id/journals/ijcls/article/view/28795.

Sucitrawan, I Nyoman, M Arief Amrullah, and Fanny Tanuwijaya Tanuwijaya. "Money Laundering Criminal Liability Through Crypto Asset Exchange in Indonesia." *International Journal of Law, Crime and Justice* 1, no. 3 (2024): 314–21. https://international.appihi.or.id/index.php/IJLCJ/article/view/190.

Wiraguna, Sidi Ahyar. "Metode Normatif Dan Empiris Dalam Penelitian Hukum: Studi Eksploratif Di Indonesia." *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3, no. 3 (2024). https://doi.org/10.59818/jps.v3i3.1390.